AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

HEARING ON VERIFICATION, SECURITY AND PAPER RECORDS FOR OUR NATION'S ELECTRONIC VOTING SYSTEMS

HEARING

BEFORE THE

COMMITTEE ON HOUSE ADMINISTRATION HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

SECOND SESSION

Hearing held in Washington, DC, September 28, 2006

Printed for the use of the Committee on House Administration

HEARING ON VERIFICATION, SECURITY AND PAPER RECORDS FOR OUR NATION'S ELECTRONIC VOTING SYSTEMS

HEARING ON VERIFICATION, SECURITY AND PAPER RECORDS FOR OUR NATION'S ELECTRONIC VOTING SYSTEMS

HEARING

BEFORE THE

COMMITTEE ON HOUSE ADMINISTRATION HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

SECOND SESSION

Hearing Held in Washington, DC, September 28, 2006

Printed for the Use of the Committee on House Administration



U.S. GOVERNMENT PRINTING OFFICE

31–270 WASHINGTON : 2007

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON HOUSE ADMINISTRATION

VERNON EHLERS, *Chairman*

ROBERT W. NEY, Ohio
JOHN L. MICA, Florida
CANDICE MILLER, Michigan
JOHN T. DOOLITTLE, California
THOMAS M. REYNOLDS, New York

JUANITA MILLENDER-McDONALD, California,
Ranking Minority Member
ROBERT A. BRADY, Pennsylvania
ZOE LOFGREN, California

WILL PLASTER, *Staff Director*
GEORGE SHEVLIN, *Minority Staff Director*

VERIFICATION, SECURITY AND PAPER RECORDS FOR OUR NATION'S ELECTRONIC VOTING SYSTEMS

THURSDAY, SEPTEMBER 28, 2006

HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOUSE ADMINISTRATION,
Washington, DC.

The committee met, pursuant to call, at 10:03 a.m., in room 1310, Longworth House Office Building, Hon. Vernon Ehlers (chairman of the committee) presiding.

Present: Representatives Ehlers, Ney, Doolittle, Millender-McDonald, Brady and Lofgren.

Also Present: Representative Holt.

Staff Present: Paul Vinovich, Counsel; Gineen Beach, Counsel; Peter Sloan, Professional Staff; George F. Shevlin, Minority Staff Director; Charles Tracy Howell, Minority Chief Counsel; Thomas Hicks, Minority Elections Counsel; Mathew A. Pinkus, Minority Parliamentarian, Janelle Rene Hu, Minority Professional Staff; Teri A. Morgan, Legislative Director, Office of Representative Brady; Stacey E. Leavandosky, Chief of Staff, Office of Representative Zoe Lofgren; and Joel Vanderver, Intern, Office of Representative Zoe Lofgren.

The CHAIRMAN. Good morning, ladies and gentlemen. The Committee on House Administration will come to order. First I would like to advise and request all members of our audience here today that all cellular phones, pagers, and other electronic equipment must be silent to prevent interruption of our business. So I would appreciate it if you would turn these devices off, as I have.

The committee is meeting today for a hearing on electronic voting machines and related issues. The election that will occur in just a few weeks will be the first general Federal election conducted since the Help America Vote Act of 2002, better known as HAVA, was fully implemented. That act, passed by this Congress in response to the voting system weaknesses exposed during the 2000 recount in Florida, set new standards for voting systems that were meant to make our elections more accurate and accessible.

Three billion dollars were appropriated by the Congress pursuant to HAVA, with most of these moneys being dedicated to new equipment purchases by jurisdictions, localities, counties, cities, townships, et cetera, that wanted to improve their voting systems. As a result many jurisdictions are using new equipment for the first time this year. It is no surprise that there have been a few problems.

Though HAVA did not require the adoption of any particular kind of technology, many jurisdictions purchased electronic voting

systems because they felt these systems were best able to meet the requirements of HAVA. Not surprisingly, some jurisdictions using this equipment for the first time have encountered some difficulties. Just two weeks ago, in nearby Montgomery County, Maryland polls were not able to open on time because poll workers were sent to their posts without the cards necessary to start up the electronic machines.

In the wake of this episode a column appeared in the Washington Post under the headline: If Paper Ballots Restore Trust in Elections, Let's Switch. The column noted people trust paper ballots because they are real. You can hold them in your hand and count them again if you need to.

Indeed, before it had electronic voting systems, Montgomery County used a punch system. Need we be reminded of the problems we had with that system.

I direct your attention to the screen above. The audience can look at that one, we will look at this one. This is a reminder of what we saw in the 2000 election in Florida, images of people with paper ballots. This one is a group of people staring at paper punch cards trying to figure out if they constitute a vote, and if so, for whom.

If you look at the second slide, you see how closely these ballots were being examined by groups.

And the third slide shows the extreme: putting things under the magnifying glass. You can see this man has got paper.

Now, I am not showing these to condemn paper, I am just pointing out that punch cards with paper, rather thick paper at that, have caused some serious problems. Simply saying "Let's use paper," as some people are saying, does not mean all the problems go away. We have to consider all the different aspects of it, and these pictures, as you can tell, were taken in Florida during the 2000 recount. That will go down in history, I am sure, because of the recount and the ramifications.

These images do not inspire trust and confidence either in the punch card system or in voting systems in general. As we look at this problem, it is worthwhile to remember the famous words of H.L. Mencken who once said, "For every complex problem there is an answer that is clear, simple, and wrong."

We would like to have answers that are clear and simple, but we certainly do not want wrong answers, and so we are going to proceed with this very thoroughly and deliberately to try to make sure that we have good answers that are right. Unfortunately, the problem some jurisdictions have experienced with their new systems have caused some to suggest that we should revert to a reliance on paper, the so-called "paper trail" or "paper tape." We know from painful and bitter experience that paper systems also can fail to deliver accurate results and are susceptible to manipulation.

To ignore this reality and assert that paper somehow ensures integrity or a correct result is simplistic and wrong. In fact, no voting system by itself can guarantee election integrity. The best system on earth will fail if not properly maintained, deployed and operated, and that is the key point that we have to remember.

Even though I am a physicist and I have used computers since 1957, I am not saying by virtue of these comments that paper is bad. Electronics, of course, is good. I have used that for many

years. I know that can fail too if not programmed or operated properly.

I believe the important point is to design the best system you can, but make sure you have auditability built in, whether it is paper or some other electronic device.

Our hearing will examine a range of issues related to electronic voting machines. We will hear about their problems but also about their benefits. We will also hear about the experience in one jurisdiction that tried to address the security concerns of a paperless system by requiring the machine to generate a paper trail.

This hearing is being held to educate the members and the public about these complicated issues. I hope when the hearing is over, we will have a better understanding of the problems and benefits of these new technologies. I also hope that as we look for solutions to these complicated problems, we resist the temptation to settle on answers that are clear, simple and wrong.

[The information follows:]

Opening Statement by Chairman Vernon J. Ehlers

Good morning ladies and gentleman, the Committee on House Administration will come to order. The Committee meets today for a hearing on electronic voting machines.

The election that will occur in just a few weeks will be the first general federal election conducted since the Help America Vote Act of 2002, or HAVA, was fully implemented. That Act, passed by this Congress in response to the voting system weaknesses exposed during the 2000 recount in Florida, set new standards for voting systems that were meant to make our elections more accurate and accessible.

Three billion dollars were appropriated pursuant to HAVA, with most of these monies being dedicated to new equipment purchases by jurisdictions that wanted to improve their voting systems. As a result, many jurisdictions are using new equipment for the first time this year.

Though HAVA did not require the adoption of any particular kind of technology, many jurisdictions purchased electronic voting systems because they felt these systems were best able to meet the requirements of HAVA. Not surprisingly, some jurisdictions using this new equipment for the first time have encountered some difficulties.

Just two weeks ago, in nearby Montgomery County, Maryland, polls were not able to open on time because poll workers were sent to their posts without the cards necessary to start up the electronic machines.

In the wake of this episode, a column appeared in the Washington Post under the headline, "If Paper Ballots Restore Trust in Elections, Let's Switch." The column noted – "People trust paper ballots because they're real. You can hold them in your hand and count them again if you need to."

Before it had electronic voting machines, Montgomery County used a punch card system. Need we be reminded of the problems we had with that system? I would direct your attention to the screen above. You will see there some images of people with paper ballots.

Here's one of a group of people staring at paper punch cards trying to figure out if they constitute a vote and if so for whom.
You can see this gentleman holding a ballot in his hand and trying to count it. You can see this man has "Got Paper"

These pictures, of course, were taken in Florida during the 2000 recount. Do these images inspire trust and confidence?

H.L. Mencken once said, "For every complex problem there is an answer that is clear, simple, and wrong."

Unfortunately, the problems some jurisdictions have experienced with their new systems have caused some to suggest that we should revert to a reliance on paper.

We know from painful and bitter experience, that paper systems can fail to deliver accurate results and are susceptible to manipulation. To ignore this reality, and assert that paper somehow ensures integrity is simplistic and wrong.

In fact, no voting system, by itself, can guarantee election integrity. The best system on earth will fail if not properly maintained and deployed.

Our hearing today will examine a range of issues related to electronic voting machines. We will hear about their problems, but also their benefits. We will also hear about the experience in one jurisdiction that tried to address the security concerns of a paperless system by requiring the machine to generate a paper trail.

This hearing is being held to educate the Members, and the public, about these complicated issues. I hope when the hearing is over, we will have a better understanding of the problems and benefits of these new technologies. I also hope that as we look for solutions to these complicated problems, we resist the temptation to settle on answers that are clear, simple and wrong.

The CHAIRMAN. Now I would like to ask unanimous consent that the gentleman from New Jersey, Representative Russ Holt, who is the author of a bill dealing very much with one aspect of this, be allowed to join us on the dais today and that he may be permitted to ask questions of the witnesses and enter his statement into the record. Without objection, so ordered.

[The information follows:]

Statement of Representative Rush Holt
to the
Committee on House Administration
Hearing on Electronic Voting Machines: Verification, Security, and Paper Trails
September 28, 2006

Chairman Ehlers, Ranking Member Millender-McDonald, Honored Members of the Committee, I would like to thank you for addressing the critical matter of the security of our electronic voting equipment and the integrity of the vote count. However, as I stated when I addressed you on the occasion of your hearing on the Hyde voter identification bill in June, and your hearing on the Voluntary Voting System Guidelines in July, this is a matter that urgently required attention long before now.

We must be honest with ourselves. The risks and dangers that accompany our use of electronic voting equipment are neither theoretical nor hypothetical. The problems we have experienced with this equipment are not taking place in a test lab, they are taking place in actual elections. It is nothing less than foolhardy, with the November elections mere weeks away, to take no action to ensure that the vote count in every race will be independently verifiable. As the September 20 editorial in Roll Call so succinctly put it, "[t]here's no way around it: If Nov. 7 is a mess, Congress will be to blame."

When I addressed the Committee in July, I recounted a number of irregularities that had already occurred during the primary season. The irregularities that occurred on electronic systems that counted voter verified paper ballots were able to be resolved, while the irregularities that occurred on electronic machines without voter verified paper records were not. For example it was reported that in May, in Grand Rapids Michigan, software in optical scanners erroneously gave votes to non-existent write-in candidates. Brand new machines malfunctioned in 15 of 16 townships and the town of Hastings in Barry County; in only one township, as confirmed by a hand count of the optical scan ballots, did the software count the votes accurately. In June, in Pottawattamie County, Iowa, software in optical scanners recorded votes inaccurately and a hand count of optical scan absentee ballots reversed the result. But in June, in Leflore and Jackson Counties, Mississippi, various glitches were experienced in the use of new paperless touch screen voting machines, including ballots not being properly customized for each precinct. An AP story published about the irregularities quoted a County-level political official as saying: "If a hacker comes in and hacks that program, what are we going to do then? . . .We're praying that everything will work out for us."

Those were merely a few of the numerous irregularities that have marred this year's primary season. I am submitting with this testimony a more extensive list, prepared by the voting integrity organization VotersUnite.org based upon published news accounts and sorted by state, that sets forth 18 reported instances of electronic voting irregularities in eight different states (Arkansas, Indiana, Iowa, Michigan, Mississippi, Montana, Texas and West Virginia), all of which took place between March and June of 2006. This list doesn't include the well-publicized meltdown that occurred most recently in Maryland. In the instances in which there were voter verified paper records available – such as those

in Pottawattamie County Iowa and Barry County Michigan -- the irregularities could be resolved. In the instances in which there were no voter-verified paper records, officials were – again – left to "pray" that everything would work out.

What does this all mean? According to prominent political analysts, in November, 45 Congressional races will be competitive or highly-competitive. However, the vote count in 22 of those competitive or highly competitive Congressional races will not be independently verifiable. Going to court will be virtually pointless in every one of those 22 instances. There will be no way to resolve vote-counting disputes in 22 races – no way to prove to the losers that they lost, and no way to reassure the public that the vote reflects the will of the majority.

We are plunging head first right into it. What on earth for? This works for *none* of us.

Some people tell me "you know, I basically agree with you, but it would create chaos to make a change in election procedures at this juncture." I think the evidence from the primary season show just the opposite. We are clearly in chaos.

In September 2005, the bipartisan Carter Baker Commission on Federal Election Reform recommended that "Congress should pass a law requiring that all voting machines be equipped with a voter-verifiable paper audit trail" in order to "provide a backup in cases of loss of votes due to computer malfunction." It further noted that "paper trails and ballots currently provide the only means to meet the Commission's recommended standards for transparency."

In June of this year, the non-partisan Brennan Center for Justice at New York University, working in conjunction with the National Institute of Standards and Technology, Ron Rivest of M.I.T, Howard Schmidt (former White House Cyber-Security Advisor for George W. Bush and former chief security officer for Microsoft and for eBay), and other computer security experts, released the most comprehensive and rigorous analysis to date of e-voting security risks and remedies. The Brennan Center report found that "[a]ll three [major types of] voting systems [used in the United States] have significant security and reliability vulnerabilities, which pose a real danger to the integrity of national, state, and local elections." To mitigate those risks, the report recommended a voter-verified paper record accompanied by automatic routine random audits and a ban on the use of voting machines with wireless components.

That same month, the National League of Women Voters, responding to increasing demand from its membership, issued similar recommendations in a resolution passed at its Annual Convention in June. The resolution states that the League of Women Voters "supports only voting systems that are designed so that: they employ a voter-verifiable paper ballot or other paper record, said paper being the official record of the voter's intent . . . . the paper ballot/record is used for audits and recounts . . . and routine audits of the paper ballot/record in randomly selected precincts can be conducted in every election."

My legislation, the Voter Confidence and Increased Accessibility Act of 2005 (H.R. 550), would implement all of the basic e-voting security recommendations of the Carter Baker Report, the Brennan Center Report and the League of Women Voters resolution. It would establish a uniform national requirement for:

a voter-verified paper record for every vote cast, which would serve as the vote of record;

routine random audits of a small percentage of the electronic tallies of the votes in every State, including at least one precinct in every county;

a band on the use of undisclosed software;

a ban on the use of wireless devices;

Federal funding to pay for the implementation of the paper record requirement; and

Voter verification mechanisms that are fully accessible to disabled voters, including a requirement that the entire process of verification be made accessible to disabled voters.

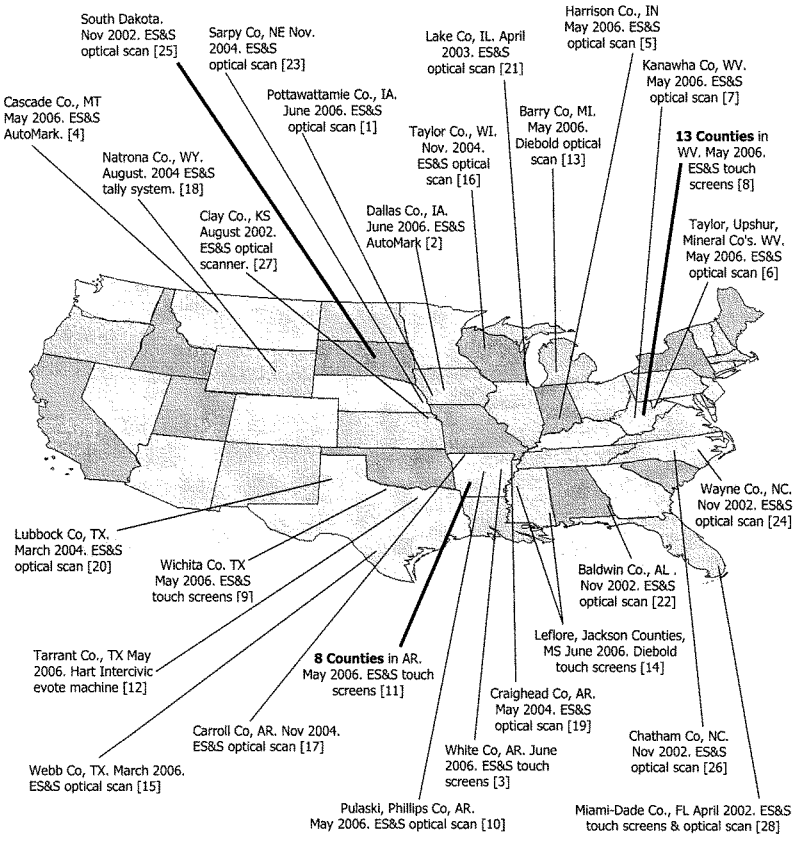
HR 550 was written to be effective in time for the November 2006 elections. You still have time to act. There are 1,050 counties in the United States that will use touch screen voting machines in November. Except for the touch screen machines used in the State of Nevada, which are equipped with voter verified paper record printers, almost none of them will be independently auditable. However, all of those counties could use absentee ballots, or emergency ballots, both of which should already be available or in the final stages of preparation in all of those jurisdictions. If you act today, those jurisdictions would have time to print enough absentee and/or emergency ballots for use by all of their voters. If they did, voters in every State, and in every Congressional race, would have the equal protection of an independently verifiable vote count in November. More importantly, we would all be able to prove to each other – winners and losers alike – who is really entitled to control of the House in the next Congress.

I thank the Committee again for giving its time and attention to this critical matter, and I urge the Committee to consider passing emergency legislation consistent with my Voter Confidence and Increased Accessibility Act as expeditiously as possible.

Vote-Switching Software Provided by Vendors

A Partial List — 51 Ballot Programming Flaws Reported in the News
These were detected; how many were not?

Ballot programming maps votes to candidates. Flaws cause votes to be counted wrong, often leaving totals unchanged. Voting machine vendors do the ballot programming for most jurisdictions in the U.S.



Detailed descriptions **www.VotersUnite.Org/info/mapVoteSwitch.pdf**

[1] **Faulty voting machines delay results; counting under way.** The Daily Nonpareil Online. June 7, 2006. Tim Rohwer, Staff Writer. http://www.zwire.com/site/news.cfm?newsid=16751509&BRD=2703&PAG=461&dept_id=555106&rfi=6

[2] **Too Much, Too Fast, More Than They Can Chew.** VoteTrustUSA. June 9, 2006. John Gideon. http://www.votetrustusa.org/index.php?option=com_content&task=view&id=1378&Itemid=51

[3] **Voters to decide candidates in runoff.** The Daily Citizen. June 12, 2006. Jeff Hunter. http://www.thedailycitizen.com/articles/2006/06/13/news/top_stories/top01.txt

[4] **Glitch, absentee votes slow results.** Great Falls Tribune. June 8, 2006. Sonja Lee, Tribune Staff Writer. http://www.greatfallstribune.com/apps/pbcs.dll/article?AID=/20060608/NEWS01/606080310/1002

[5] **Ballot-counting problem.** WHAS11.com. May 15, 2006. http://www.whas11.com/topstories/stories/WHAS11_TOP_ballotcounting.42e3d88f.html

[6] **Several Counties Have Vote Counting Problems.** WOWKTV 13. May 10, 2006. Dave Kirby. http://wowktv.com/story.cfm?func=viewstory&storyid=10787

[7] **Kanawha's dry run of voting machines remains incomplete.** Charleston Gazette. May 03, 2006. Archive http://www.votersunite.org/article.asp?id=6596

[8] **Election test delayed.** TMCnet. May 1, 2006. by Charleston Gazette writer Phil Kabler and AP. http://www.tmcnet.com/usubmit/2006/05/01/1628275.htm

[9] **Vendor bender. City clerk blames ES&S for Election Day difficulties.** Times Record News. May 14, 2006. Robert Morgan. Archived at http://www.votersunite.org/article.asp?id=6598

[10] **Recount Planned In Close Race For State House Nomination.** Todays THV. June 2, 2006. http://www.todaysthv.com/news/news.aspx?storyid=29413

[11] **Eight counties won't use electronic equipment in runoff.** The Log Cabin Democrat. June 9, 2006. by Andrew DeMillo, AP. http://ap.thecabin.net/pstories/state/ar/20060609/4000271.shtml

[12] **Ballot problems mark 1st day of early voting.** Star-Telegram. May 2, 2006. Neil Strassman. http://www.dfw.com/mld/dfw/news/local/14479735.htm

[13] **Malfunction delays Hasting results.** The Grand Rapids Press. May 04, 2006. By Ben Cunningham. http://www.mlive.com/news/grpress/index.ssf?/base/news-0/1146754492135040.xml&coll=6

[14] **Most voting goes smoothly. A few glitches in primary, not serious.** Sun Herald. June 7, 2006. By Shelia Byrd, AP. http://www.sunherald.com/mld/sunherald/news/state/14758095.htm

[15] **Election Uproar; County officials say there were plenty of red flags.** Laredo Morning Times, March 14, 2006 by Julie Daffern. http://www.zwire.com/site/index.cfm?newsid=16299334&BRD=2290&PAG=461&dept_id=473478&rfi=8

[16] **About 600 Medford ballots cast in November ignored.** Mar 12, 2005. Marshfield News-Herald. http://www.wisinfo.com/newsherald/mnhlocal/28404948565692 6.shtml

[17] **Computer glitch blamed for miscount in JP voting.** Carroll County Star Tribune. November 10, 1004. By Anna Mathews. Reproduced at http://www.votersunite.org/article.asp?id=3889

[18] **Clerk changes election vote totals.** Star-Tribune. August 21, 2004. By Matthew Van Dusen, staff writer. http://www.casperstartribune.net/articles/2004/08/21/news/casper/6c2e825b3f9e154187256ef70007adbb.txt

[19] **Commission OKs results of elections.** Jonesboro Sun, May 28, 2004. By LeAnn Askins. http://www.jonesborosun.com/archivedstory.asp?ID=9486

[20] **Software blamed in Precinct 8 Democratic chair race mixup.** Lubbock online.com; March 11, 2004; By Brian Williams, Avalanche-Journal. http://www.lubbockonline.com/stories/031104/loc_031104030.shtml

[21] **Returns are in: Software goofed — Lake County tally misled 15 hopefuls.** Chicago Tribune; April 4, 2003; By Susan Kuczka, Tribune staff reporter. Reproduced at http://www.vote.caltech.edu/mail-archives/votingtech/Apr-2003/0096.html

[22] **Voting snafu answers elusive.** The Mobile Register; 28 Jan 2003; by Brendan Kirby, staff writer. Referenced at http://www.votewatch.us/Members/Unregistered%20User/ electionexperience.2004-08-12.9166974619

[23] **A late night in Sarpy; glitches delay results.** Omaha World-Herald, 6 November 2002; Referenced in *Black Box Voting*, by Bev Harris. Chapter 2.

[24] **Winners' may be losers.** The News and Observer; November 12, 2002; By Wade Rawlins and Rob Christensen.

[25] **Analysis: Senate races in Minnesota and South Dakota.** NPR: Morning Edition, 6 November 2002; Ref. in Black Box Voting by Bev Harris, Chapter 2.

[26] **Mechanic to smooth vote.** New Observer. October 15, 2004. By Jessica Rocha, Staff Writer. http://newsobserver.com/news/story/1730333p-7996316c.html

[27] **Aug. 6 ballot problems alleged: Clay, Barton county candidates seek review of races.** Lawrence Journal-World. August 22, 2002. AP. http://www.ljworld.com/section/election02/story/103526

[28] **Technician's Error, Not Machines, To Blame In Dade Election Mix-Up.** The Miami Herald. April 4, 2002. By Oscar Corral.

Vote-Switching Software Provided by Vendors — A Partial List Reported in the News

Ballot programming maps votes to candidates. Flaws cause votes to be counted wrong, often leaving totals unchanged.
Voting machine vendors do the ballot programming for most jurisdictions in the U.S.

(Map Handout)

Map#	Date	Machine	State	Place/Description
22	November 2002	ES&S Optech 3P Eagle	**Alabama**	**Baldwin County, Alabama.** Tabulation machine initially handed the gubernatorial election to the wrong candidate. Initial, unofficial results from Baldwin County showed that Democrat Don Siegelman garnered about 19,070 votes in the county, enough to give him a razor-thin victory over Republican challenger Bob Riley. The next morning, however, officials said those totals were inaccurate and certified returns giving Siegelman about 6,300 fewer votes -- enough to swing the election to Riley. ... Officials have traced the problem to a data pack from the Magnolia Springs voting location. They said the vote-counting machine there printed out accurate results when the polls closed at 7 p.m. But they said the cartridge, which resembles an eight-track cassette, gave bogus figures when it was plugged into the computer in Bay Minette. [1]
3	June 2006	ES&S iVotronic	**Arkansas**	**White County, Arkansas.** ES&S provides flawed ballot programming for the touch screens.[2] After initial problems with the county's new iVotronic electronic voting machines -- including faulty electronic ballots, that forced the use of homemade paper ballots in early voting — White County Clerk Tanya Burleson said ballots in today's runoff will be cast electronically as originally planned.
10	May 2006	ES&S Optical scanner	**Arkansas**	**Pulaski County and Phillips County, Arkansas.** ES&S provided flawed ballot programming in both counties.[3] Daniels said that in Pulaski and Phillips counties, the problems involved old optical scanners that were not programmed adequately to count paper ballots in the election. Initial count showed a tie for House District 41, with both candidates getting 613 votes. The recount showed 655 to 664.

[1] **Voting snafu answers elusive.** The Mobile Register; 28 Jan 2003; by Brendan Kirby, staff writer. Referenced at http://www.votewatch.us/Members/Unregistered%20User/electionexperience.2004-08-12.9166974619. Confirmed by VotersUnite! with Sharon Jerkins in the Baldwin County Elections office, who provided the model number of the optical scan machines.

[2] **Voters to decide candidates in runoff.** The Daily Citizen. June 12, 2006. By Jeff Hunter. http://www.thedailycitizen.com/articles/2006/06/13/news/top_stories/top01.txt

Vote-Switching Software Provided by Vendors — A Partial List Reported in the News

Map#	Date	Machine	State	Place/Description
11	May 2006	ES&S iVotronic	**Arkansas**	**Arkansas.** Ballot programming errors were found on iVotronics touch screens in **eight** counties before the election.[4] Pulaski County Elections Director Susan Inman said that county decided not to use the machines after reviewing the programming code from voting machine vendor Election Systems & Software and discovering errors. "In its entirety, it was wrong," Inman said. "I forwarded to them in time for the deadline I was given the information for the runoff." 72 of 75 counties are have ES&S equipment. 64 still used iVotronics in the election.
17	November 2004	ES&S Optical scan	**Arkansas**	**Carroll County, Arkansas.** A mis-programmed chip from ES&S skewed the results from the JP District 2 race. [5] The glitch was discovered by Carroll County Election Commission members when they met to certify election results Monday at the Berryville courthouse. It is believed that the programming alignment was out of kilter, as provided by Election Systems and Software, the company that programs computer chips to read the local ballots. As a result, ballots for the JP District 2 race will either be hand counted, or re-run through the optical scanner machine once the correct computer chip is provided.

[3] **Recount Planned In Close Race For State House Nomination.** Todaysthv.com. June 2, 2006. http://www.todaysthv.com/news/news.aspx?storyid=29413

[4] **Election Problems Persist For Eight Counties.** Today's THV. June 8, 2006. http://www.todaysthv.com/news/news.aspx?storyid=29699

Eight counties won't use electronic equipment in runoff. The Log Cabin Democrat. June 9, 2006. by Andrew DeMillo, Associated Press Writer. http://ap.thecabin.net/pstories/state/ar/20060609/4000271.shtml

[5] **Computer glitch blamed for miscount in JP voting.** Carroll County Star Tribune. November 10, 1004. By Anna Mathews. Reproduced at http://www.votersunite.org/article.asp?id=3889

Vote-Switching Software Provided by Vendors — A Partial List Reported in the News

Map#	Date	Machine	State	Place/Description
19	May 2004	ES&S Optical scanner (possibly Model 150)	**Arkansas**	**Craighead County, Arkansas.** The chip programmed by ES&S for the county's optical scanner gave one candidate all the votes for constable. A manual recount revealed the error. A recount was made in the District 13 constable race because returns from Precinct 20 showed one candidate received all 158 votes cast in the precinct, and the opposing candidate doubted that. The incident was traced back to a computer chip coding error, and the result of the recount was that both candidates had received votes in the precinct. [6]
n/a	June 2006	ES&S Optical scan	**Arkansas**	**St. Francis County, Arkansas.** A recount of the State Senate District 16 runoff primary race reversed the initial, incorrect results caused by a ballot programming error.[7] Results in the Senate District 16 originally showed Representative Arnell Willis of Helena-West Helena defeating Earle School Superintendent Jack Crumbly by 28 votes. However, a recount in St. Francis County on Monday gave Crumbly 100 more votes, making him the winner. Election officials had said earlier that a tabulation error had resulted in 100 fewer votes being counted for Crumbly. St. Francis County Election Commission Chairman Frederick Freeman apologized to the candidates.

[6] **Commission OKs results of elections.** Jonesboro Sun, May 28, 2004. By LeAnn Askins. http://www.jonesborosun.com/archivedstory.asp?ID=9486

[7] **Recount In AR Race Reverses Result.** Eyewitness News. June 20, 2006. http://www.myeyewitnessnews.com/news/local/story.aspx?content_id=3734B371-B2D5-416C-9A72-D1AF88685953. Archive: http://www.votersunite.org/article.asp?id=6606

Vote-Switching Software Provided by Vendors — A Partial List Reported in the News

Map#	Date	Machine	State	Place/Description
n/a	May 2006	ES&S Optical scan	**Arkansas**	**Phillips County, Arkansas.** Tabulators, with flawed ballot programming furnished by ES&S, mistook 432 Democratic votes for Republican and fail to count them in the Democratic primary. [8] Several days after the Election Commission certified that race and Crumbly and Willis began campaigning for the June 13 runoff, commission staff discovered that 432 votes cast at Allen Temple in Phillips County had mistakenly been counted as Republican ballots, effectively nullifying them. The malfunctioning ballot tabulating machine was programmed by Election Systems & Software, the Omaha, Neb.-based company that in November signed a $ 15 million contract to provide election equipment to Arkansas counties. Ballot programming problems in Phillips County also affected the House District 41 contest. [9]
n/a	May 2004	Optical scanner (possibly Model 150)	**Arkansas**	**Fulton County, Arkansas.** The chip programmed by ES&S for the county's optical scanner didn't work. ES&S claimed that the printer didn't send them all 16 ballots needed for the programming. The printer said he did send the entire set of ballots, and his records showed that the weight of the package mailed to ES&S was the weight of 16 ballots. [10] Riverside Graphics printer Michael Eaton insisted his company sent ESS [sic] a full set of ballots. "We printed the ballots for Independence County where there are three times as many people and we didn't have any problems. We've had this problem with ESS before," said Eaton. ... He said Riverside Graphics checked its postage records, and the weight of the package sent to ESS was consistent with a package containing 16 ballots.

[8] **District 16 recount sought; 432 lost votes cited in suit.** Northwest Arkansas News Source, June 24, 2006. BY DANIEL NASAW. http://www.nwanews.com/adg/News/158589/. Archive: http://www.votersunite.org/article.asp?id=6605

[9] **Vendor bender. City clerk blames ES&S for Election Day difficulties.** Times Record News. May 14, 2006. By Robert Morgan. http://www.votersunite.org/article.asp?id=6598

[10] **No explanation for ballot machine malfunction.** South Missourian; May 27, 2004; by George Jared, Staff Writer

Vote-Switching Software Provided by Vendors — A Partial List Reported in the News

Map#	Date	Machine	State	Place/Description
n/a	May 2004	Model 150	**Arkansas**	**Sevier County, Arkansas.** The chip programmed by ES&S counted all ballots as blank. The test ballots were printed correctly, and the pre-election testing was successful. But then the ballots for election day were printed in a completely different print run, and the codes on these election-day ballots didn't match the codes on the computer chip prepared by ES&S. [11] After consulting with officials from Election Systems & Software, it was determined that the codes on the computer chip and the codes on the ballot didn't match.
n/a	August 2004	Sequoia Veri-Vote	**California**	**Sacramento, California.** In a demonstration of its Direct Recording Electronic voting machine with a paper trail, Sequoia demonstrated that its machine failed to report four votes in Spanish.[12] Last week, Sequoia vice president and former California assistant secretary of state Alfie Charles was showing off the new Veri- Vote printer that his firm is supplying to Nevada when an astute legislative aide in Johnson's office noticed two votes were missing. Charles tried again to vote in Spanish with the same result: He cast votes on two mock ballot initiatives, but they were absent from the electronic summary screen and the paper trail. "The paper trail itself seemed to work fine but what it revealed was when he demonstrated voting in Spanish, the machine itself did not record his vote," Chesin said. "Programming errors can occur and the paper trail was the way we caught it."
n/a	March 2004	Diebold AccuVote optical scan	**California**	**San Diego, California.** Optical scan machines counted 208,446 ballots. The machines miscounted 2,821 votes in the Democratic presidential race and the Republican U.S. Senate seat. [13] Most of the absentee miscounts occurred in the Democratic presidential race, in which 2,747 votes cast for John Kerry were incorrectly credited to Rep. Dick Gephardt. In the Senate race, in which Bill Jones won, 68 votes cast for Barry L. Hatch were credited to candidate Tim Stoen, and six votes cast for James Stewart were credited to Stoen. [14]

[11] **Ballots counted by hand in primary elections.** The DeQueen Bee; May 24, 2004. http://www.dequeen.com/news/comments.php?id=1188_0_1_0_C

[12] **Lawmakers cut e-voting's paper trail: Manufacturers demonstrating new printers in Nevada were embarrassed when machine failed to recognize votes.** Tri-Valley Herald. August 13, 2004. By Ian Hoffman, Staff Writer. Reproduced at: http://www.votersunite.org/article.asp?id=2512

Wrong Time for an E-Vote Glitch. Wired News. August 12, 2004. By Kim Zetter. http://www.wired.com/news/evote/0,2645,64569,00.html?tw=wn_tophead_2

Vote-Switching Software Provided by Vendors — A Partial List Reported in the News

Map#	Date	Machine	State	Place/Description
28	April 2002	iVotronic and optical scanners	**Florida**	**Miami-Dade County, Florida.** In Medley, the software used to combine 45 absentee votes with the 309 electronic ballots changed the order of the candidates' names as it computed the results. The initial tally showed wins for two City Council candidates who actually lost the election. David Leahy, Miami-Dade **elections** supervisor said that all software had been tested before the election without a problem. Election workers who had been watching the results fed into the computer noticed the problem. **The tabulation computer didn't give any warning.** An ES&S technician had opened the ballot program on the memory cards to change a header. At the same time, he bumped the first candidate to the last position. When the technician saved the edit, a prompt most likely popped up on the monitor asking him if he was sure he wanted to change the order of the names. The technician ignored the prompt and confirmed the change. "It was something that should have been picked up and caught and was missed and was not flagged because the normal follow-up procedures to making a change in the database were not followed," [Mike] Limas [ESS Chief Operating Officer] said. ... Leahy said he is concerned because the computer did not raise any red flags, and humans had to spot the error. "If something is amiss you should get some type of error message, but there wasn't one," he said. ... In the future, Leahy said county election workers, not technicians from the equipment company, will program all the touch-screen and absentee ballot machines before an election to try to limit the possibility of error. He also suggested that humans might add up the absentee ballots with the touch-screen voting results to double check the computer's tally. [15]

[13] **New electronic scanners miscounted some county votes.** NC Times April 7, 2004; By: Gig Conaughton - Staff Writer; http://www.nctimes.com/articles/2004/04/08/news/top_stories/22_27_394_7_04.txt

[14] **Some votes miscounted in primary, officials say**. Union-Tribune. April 8, 2004. By Luis Monteagudo Jr. and Helen Gao, staff writers. http://www.signonsandiego.com/news/politics/20040408-9999-1m8vote.html

[15] **Technician's Error, Not Machines, To Blame In Dade Election Mix-Up.** The Miami Herald. April 4, 2002. By Oscar Corral. [Purchase through Miami Herald online archives: http://www.miami.com/mld/miamiherald/archives/]

Vote-Switching Software Provided by Vendors — A Partial List Reported in the News

Map#	Date	Machine	State	Place/Description
n/a	September 2002	Optical scan	**Florida**	**Union County, Florida.** [16] In Union County, Florida, a programming error caused machines to read 2,642 Democratic and Republican votes as entirely Republican in the September 2002 election. The vendor, ES&S, accepted responsibility for the programming error and paid for a hand recount.
n/a	March 2002	AVC Edge	**Florida**	**Palm Beach County, Florida.** Former Boca Raton Emil Danciu was ahead by 17 points in a poll conducted by the opposition. Exit polling indicated an overwhelming win for Danciu, but he received only 19% of the votes, even losing in his home precinct. Voters report that their votes appeared to be registered for his opponent. "What really alarmed us was the next day when we started getting phone calls from voters who had gone into the voting places -- people we didn't even know -- and pushed Emil Danciu's name only to end up with a check mark by Susan Haynie's name. They repeatedly tried to vote for him, but another name, particularly Haynie's, came up. They couldn't get their vote registered. They were telling wild stories about poll workers unplugging and kicking the machines. They didn't know whether their votes ever counted. Some were told to vote again." [17] In addition, the results were delayed because, according to the election supervisor's office, 15 cartridges had been lost, and the system won't give a final tally until it has read all the cartridges. The office said that a poll worker had taken them home, and then they found them. With no paper ballots to check the accuracy of the machine, Danciu sued for the right to look at Sequoia source code. The county attorney argued that it would be a felony to disclose the source because it is a trade secret. The judge denied Danciu's request for the software code. [18]

[16] **Black Box Voting** by Bev Harris, Chapter 2.

[17] **Out of Touch: You press the screen. The machine tells you that your vote has been counted. But how can you be sure?** New Times; April 24, 2003; By Wyatt Olson. http://www.newtimesbpb.com/issues/2003-04-24/feature.html/1/index.html

[18] **Electronic voting's hidden perils.** Mercury News. February 1, 2004. By Elise Ackerman. http://www.mercurynews.com/mld/mercurynews/news/special_packages/election2004/7849090.htm

Vote-Switching Software Provided by Vendors — A Partial List Reported in the News

Map#	Date	Machine	State	Place/Description
21	April 2003	ES&S Model 100 optical scan	**Illinois**	**Lake County, Illinois.** [19] Machines provided incorrect outcomes for 4 races in Lake County. The problem was caused by a programming error that failed to account for "no candidate" listings in some races on the ballot, Clerk Willard Helander said Thursday. As a result, election results were placed next to the names of the wrong candidates in four different races, including in Waukegan's 9th Ward. Incorrect results also were tabulated in races for the Libertyville Community High School District 128 Board, the North Chicago Community Unit District 187 Board and the Foss Park District Board in North Chicago. The clerk's office corrected the problem shortly after 10 p.m. on election night. But by then, many people who had kept track of the results on the clerk's online Web site believed the unofficial results were complete. ... Helander blamed the problem on Election Systems & Software, the Omaha company in charge of operating the county's optical-scan voting machines. She said a company official told her the programmers were unaware the county would have "no candidate" listings on its ballot.
5	May 2006	ES&S Optical scanner	**Indiana**	**Harrison County, Indiana.** Flawed ballot programming errors by ES&S were detected in the testing on ES&S optical scanners.[20] Time didn't allow the revised programming to be tested. Programming errors in automatic tabulation equipment connected to voting machines were discovered by county officials before and during the primary. After the problems were discovered during a routine test before the election, county officials returned some of the equipment to the Omaha company for reprogramming, but there wasn't time before the primary to perform a second test, said AJ Feeney-Ruiz, a spokesman for Secretary of State Todd Rokita.

[19] **Returns are in: Software goofed — Lake County tally misled 15 hopefuls.** Chicago Tribune; April 4, 2003; By Susan Kuczka, Tribune staff reporter reproduced at http://www.vote.caltech.edu/mail-archives/votingtech/Apr-2003/0096.html

[20] **Ballot-counting problem.** WHAS11.com. May 15, 2006. http://www.whas11.com/topstories/stories/WHAS11_TOP_ballotcounting.42e3d88f.html

Vote-Switching Software Provided by Vendors — A Partial List Reported in the News

Map#	Date	Machine	State	Place/Description
1	June 2006	ES&S Optical Scan (M-100)	Iowa	**Pottawattamie County, Iowa.** Ballot programming error by ES&S causes new optical scanners to tabulate votes incorrectly. [21] Things began to look fishy, [Pottawattamie County Auditor Marilyn Jo] Drake said, when the county's new computers counted the absentee ballots in the Republican Party's county race between longtime Recorder John Sciortino and newcomer Oscar Duran. Absentee ballots are the ones counted first. When all of those were counted, Duran, a University of Nebraska at Omaha student, had 99 votes, while Sciortino, the county recorder since 1983, had just 79. ... Drake said she decided to count the absentee ballots by hand to determine if the computers were counting correctly. They weren't - not by a long shot. The actual absentee ballot count in the recorder's race when done by hand found Sciortino had 153 votes and Duran just 25. It was then that she decided to stop the computer counting in all the races. "They could be tainted, we don't know," Drake said.
2	June 2006	ES&S AutoMark	Iowa	**Dallas County, Iowa.** ES&S mis-programmed the ballots on the AutoMark. The review screen didn't match the marks on the paper ballot. [22] [Charles Krogmeier of the Secretary of State's staff] told VoteTrustUSA that a professor from Drake University asked to use the AutoMark machine when he voted. He went through the ballot, marking his choices, and when he was through he checked the ballot to find that one race had been swapped.

[21] **Faulty voting machines delay results; counting under way.** The Daily Nonpareil Online. June 7, 2006. by Tim Rohwer, Staff Writer. http://www.zwire.com/site/news.cfm?newsid=16751509&BRD=2703&PAG=461&dept_id=555106&rfi=6

[22] **Too Much, Too Fast, More Than They Can Chew.** VoteTrustUSA. June 9, 2006. By John Gideon. http://www.votetrustusa.org/index.php?option=com_content&task=view&id=1378&Itemid=51

Vote-Switching Software Provided by Vendors — A Partial List Reported in the News

Map#	Date	Machine	State	Place/Description
n/a	June 2006	ES&S Optical Scan (M-100)	**Iowa**	**Pottawattamie County, Iowa.** Flawed ballot programming by ES&S reported results of all nine contested primary races incorrectly. [23] Pottawattamie County elections deputy Gary Herman said anomalies were noticed almost immediately. Electronic results were posted, but with a disclaimer that ballots would be hand-counted the next day. The results were dramatic. **Every winner in Pottawattamie County's nine contested races turned out, in retrospect, to be a loser.** Initial returns that showed incumbent Recorder John Sciortino losing by a margin of 1,245 votes to 1,167 was found to have actually won the election 2,061 votes to 347.
27	August 2002	ES&S Central count optical scan	**Kansas**	**Clay County, Kansas.** The machine showed that the challenger (Jennings) had won, but a hand recount showed that the incumbent commissioner (Mayo) won by a landslide — 540 votes to 175. In one ward, which Mayo carried 242-78, the computer had mistakenly reversed the totals. [24] This statement indicates that the computer in the "one ward" had the candidates mis-mapped to the table that holds the voting results.
13	May 2006	Diebold AccuVote OS	**Michigan**	**Barry County, Michigan.** Diebold delivers flawed ballot programming, which tallied votes incorrectly. [25] Hastings Clerk Thomas Emery saw the problem immediately after receiving the roll from the precinct where he had voted. "The person I voted for had zero votes, and I know how to fill in an oval," he said. Emery voted for the candidate on the top line of the ballot. The fourth line of the ballot -- reserved for write-in candidates -- accumulated 90 votes from only 127 ballots cast at the precinct. "I knew for certain there wouldn't be 90 write-ins," Emery said.

[23] **Polk County recorder to contest election.** The Des Moines Register, June 24, 2006. Bert Dalmer, Register Staff Writer. http://desmoinesregister.com/apps/pbcs.dll/article?AID=/20060624/NEWS05/606240322/1001. Archive: http://www.votersunite.org/article.asp?id=6607

[24] **Aug. 6 ballot problems alleged: Clay, Barton county candidates seek review of races.** Lawrence Journal-World. August 22, 2002. The Associated Press. http://www.ljworld.com/section/election02/story/103526

[25] **Malfunction delays Hasting results.** The Grand Rapids Press. May 04, 2006. By Ben Cunningham. http://www.mlive.com/news/grpress/index.ssf?/base/news-0/1146754492135040.xml&coll=6

Vote-Switching Software Provided by Vendors — A Partial List Reported in the News

Map#	Date	Machine	State	Place/Description
14	June 2006	Diebold AccuVote TS	**Mississippi**	**Leflore, Jackson Counties, Mississippi.** Ballot programming by Diebold was incorrect on touch screens in these two counties.[26] In Leflore and Jackson counties, early voters had to cast paper ballots because the touch-screen machines were not customized for each precinct, said David Blount, spokesman for Secretary of State Eric Clark. The machines were fixed by Tuesday afternoon, he said. The problems prompted the Leflore County election commissioners to petition the Board of Supervisors for their own technician.[27] Diebold Election Systems, as part of its contract, will offer assistance to the county for five years. But the county's difficulties during the June 6 primary were due to improper programming by a Diebold technician. These problems prompted the commission's request.
4	May 2006	ES&S AutoMark	**Montana**	**Cascade County, Montana.** Programming problems occurred with the new AutoMark system.[28] Clerk and Recorder Peggy Carrico said most of the systems worked, although the AutoMark in Belt was shut down because of a programming problem.
23	November 2002	ES&S Optical scan	**Nebrask**	**Sarpy County, Nebraska.** The optical scan machines failed to tally "yes" votes on the Gretna school-bond issue, giving the false impression that the measure failed miserably. The measure actually passed by a 2-1 margin. Responsibility for the errors was attributed to ES&S, which provided the ballots and the machines. [29]

[26] **Most voting goes smoothly. A few glitches in primary, not serious.** Sun Herald. June 7, 2006. By Shelia Byrd, AP.
http://www.sunherald.com/mld/sunherald/news/state/14758095.htm

[27] **Voting Machines.** The Greenwood Commonwealth. June 28, 2006. By Susan Montgomery.
http://www.zwire.com/site/news.cfm?newsid=16858105&BRD=1838&PAG=461&dept_id=104621&rfi=6

[28] **Glitch, absentee votes slow results.** Great Falls Tribune. June 8, 2006. By SONJA LEE, Tribune Staff Writer.
http://www.greatfallstribune.com/apps/pbcs.dll/article?AID=/20060608/NEWS01/606080310/1002

[29] **Omaha World-Herald,** 6 November 2002; "A late night in Sarpy; glitches delay results". Referenced in *Black Box Voting*, by Bev Harris. Chapter 2.

Vote-Switching Software Provided by Vendors — A Partial List Reported in the News

Map#	Date	Machine	State	Place/Description
n/a	November 2004	Optical Scan	Nebraska	**Lancaster County, Nebraska.** As the optical scanners read the election-day ballots, occasionally, they added votes. While County Election Commissioner David Shively explained that the software was reading ballots twice, ES&S referred to the misread as a mechanical problem. [30] Inexplicably, both Shively and the Nebraska deputy secretary of state for elections, Neal Erickson, agreed that "the malfunctions were not the type that taint vote counts." The problem, described by Shively: While machines correctly fed themselves just one ballot at a time, their software at times incorrectly detected two ballots. The machines in all cases stopped short of actually counting two ballots, Shively said, and instead responded by shutting down. ... Shively said it became clear after 2 p.m. Tuesday that problems existed. At that time, officials began testing the six machines — four for election-day ballots, two on loan from Election Systems & Software to count absentee ballots — and found that two were not correctly matching results. That came as a surprise, Shively said, because all were tested late last week and performed well. After consulting with ES&S, Shively decided to use the two absentee-ballot machines to speed up the election-day counting. But the problem was apparently contagious. From about 10:30 p.m. to 12:30 a.m., the machines were purring along glitch-free, Shively said. "I thought, 'Boy, we're back in business,'" Shively said. **Then the two-ballot problem described by Shively began, plaguing almost all the machines,** drastically slowing the count.

[30] **Problem machines spur call for recount.** Lincoln Journal Star. November 14, 2004. By Nate Jenkins. http://www.journalstar.com/articles/2004/11/14/election/doc4189b9c7f14bf764391458.txt

Vote-Switching Software Provided by Vendors — A Partial List Reported in the News

Map#	Date	Machine	State	Place/Description
n/a	November 2004	Optical Scan	**Nebraska**	**Sarpy County, Nebraska.** Election officials ended up with around 10,000 phantom votes (more votes than voters). They still don't know what went wrong. [31] Johnny Boykin lost his bid to be on the Papillion City Council. The difference between victory and defeat in the race was 127 votes. Boykin says, "When I went in to work the next day and saw that 3,342 people had shown up to vote in our war, I thought something's not right." He's right. There are not even 3,000 people registered to vote in his ward. For some reason, some votes were counted twice. Deputy Sarpy County Election Commissioner Ed Gilbert says, "It affected 32 of the 80 precincts. And I suppose as many as 10,000 votes." ... No one is sure exactly what went wrong. Astonishingly, election officials are projecting a winning candidate based on the assumption that the votes were counted twice and that the outcome wouldn't be affected. Election officials say they don't believe the glitch will impact who won and who lost any of the races. They figure that when votes were doubled in a particular race, the totals were doubled for both candidates. Vote totals would be skewed but percentages would not change. In spite of that, the candidates want to know the real numbers. VotersUnite contacted the Sarpy County Elections office and was told that ES&S had analyzed the problem and determined it to be "mechanical and procedural." That was all the election staff knew.
n/a	November 2002	Optical scan	**Nebraska**	**Adams County, Nebraska.** During the general election, Adams County was the last in Nebraska to have election results, due to both machine and software malfunctions. ES&S talked about some compensation for the election problems including paying for election worker overtime and not charging for **programming adjustments.** [32]

[31] **Countinghouse Blues: Too many votes.** WOWT Omaha. November 5, 2004. http://www.wowt.com/news/headlines/1161971.html

[32] YorkNewsTimes.com, December 20, 2002; "**Omaha election systems firm to pay for county election problems**." Referenced in *Black Box Voting*, by Bev Harris. Chapter 2.

Vote-Switching Software Provided by Vendors — A Partial List Reported in the News

Map#	Date	Machine	State	Place/Description
n/a	November 2002	Sequoia optical scan	**New Mexico**	**Taos, New Mexico.** A software programming error caused the Sequoia Optech optical scanner to assign votes to the wrong candidates. Just 25 votes separated the candidates in one race; another race had a 79-vote margin. After noticing that the computer was counting votes under the wrong names, Taos County Clerk Jeannette Rael contacted the programmer of the optical machine and was told it was a programming error.[33]
n/a	November 2000	Diebold AccuVote OS	**New Mexico**	**Bernalillo County, New Mexico.** Flawed ballot programming for the presidential election caused 67,000 absentee and early-voting ballots to be counted incorrectly. The panicked officials first thought computerized tabulation machines or balloting software were at fault. The county uses the AccuVote optical scan system from Global Election Systems Inc. of McKinney, Texas. The tabulation system and software worked correctly, but a county technical employee failed to set up an element of the system properly, said Frank Kaplan, Global's Western regional manager. New Mexico's ballots are designed for voting by party, but voters can choose candidates from other parties. A programmer did not link the candidates' names to their respective parties.[34]
24	November 2002	Optech Eagle	**North Carolina**	**Wayne County, North Carolina.** A programming error caused the Optech Eagle optical scan machines to skip several thousand party-line votes, both Republican and Democrat. Correcting the error turned up 5,500 more votes and reversed the outcome for the House District 11 state representative race. [35]

[33] 06/03/04. Conversation with a woman at the Elections Division of New Mexico. She told me Taos used the Sequoia Optech and confirmed that it was a programming error by the local programmer. New Mexico does not have their ballot programming done by the vendor. Original reference from *Black Box Voting*, Chapter 2. Albuquerque Journal, 7 November 2002; **"Taos To Recount Absentee Ballots"**

[34] **Human error is cause of N.M. election glitch.** Government Computer News; November 20, 2000; Vol. 19 No. 33 http://www.gcn.com/vol19_no33/news/3307-1.html

[35] **"Winners' may be losers."** The News and Observer; November 12, 2002; By Wade Rawlins and Rob Christensen.

Vote-Switching Software Provided by Vendors — A Partial List Reported in the News

Map#	Date	Machine	State	Place/Description
26	November 2002	ES&S Optech 3P	**North Carolina**	**Chatham County, North Carolina.** A ballot programming error caused Republican votes to go to the Libertarian candidate. [36] ... every time voters marked a straight Republican ticket, Frederick C. Blackburn, the N.C. House 54 Libertarian candidate, got a vote because of a voting machine programming error.
n/a	September 2002	Optical scan	**North Carolina**	**Robeson County, North Carolina.** Ballot tabulating machines failed to work properly in 31 of 41 precincts. Local election officials said the problem was the result of a software glitch, and ballots had to be recounted. There had been a problem in the programming of the memory cards. [37]
n/a	November 2005	ES&S optical scanner	**Pennsylvania**	**Cumberland County, Pennsylvania.** Flawed ballot programming of straight-ticket votes hands the race to the wrong candidate for magisterial district judge. Straight-ticket Democrat votes were given to the Republican candidate. Straight-ticket Republican votes were not counted at all.[38] A 9.5-hour hand recount produced a new winner Thursday in the election for magisterial district judge for the Carlisle area. ...Democrat Jessica Rhoades came out on top by a slim two-vote margin — 1,703-1,701 — over Republican Kathy Keating in the recount. Initial vote totals recorded Tuesday night showed Keating won by a 1,650-1,468 margin. However, a programming error by the county's ES&S voting machines awarded all votes by Democrats casting a straight-ticket ballot to Keating. The problem involved a software coding error in which Keating's political affiliation was mislabeled as Democrat. Straight-ticket Republican votes were not awarded to either candidate. So the hand recount subtracted straight-ticket Democrat votes from Keating's total and added straight-ticket Republican votes. Meanwhile, Rhoades gained straight-ticket Democrat votes.

[36] **Mechanic to smooth vote.** New Observer. October 15, 2004. By Jessica Rocha, Staff Writer. http://newsobserver.com/news/story/1730333p-7996316c.html

[37] January 2004 Conversation with Dinah in the Robeson County Clerk's office. Original reference was "Voter turnout surprises officials." Sun News. September 12, 2002. http://www.myrtlebeachonline.com/mld/sunnews/news/local/4056664.htm

[38] **DJ race still up in the air.** Sentinel, November 11, 2005. By John Hilton. http://www.cumberlink.com/articles/2005/11/11/news/news02.txt Archive: http://www.votersunite.org/article.asp?id=6323

Vote-Switching Software Provided by Vendors — A Partial List Reported in the News

Map#	Date	Machine	State	Place/Description
25	November 2002	ES&S Optech 4C	South Dakota	**South Dakota.** When the optical scanner double counted votes, the error was blamed on a "flawed chip." ES&S sent a replacement chip, and voters demanded that the original chip be impounded and examined. Only ES&S was allowed to examine the chip. [39]
9	May 2006	ES&S iVotronic	Texas	**Wichita Falls, Texas.** ES&S provided flawed programming for the touch screens.[40] And according to City Clerk Lydia Ozuna the blame rests firmly on the shoulders of Election Systems and Software, the county's election vendor. ... Besides a delay in ballot counting, Ozuna said she had received calls about difficulties with the electronic voting machines. Poll workers called in saying the machines were not working properly. Ozuna said she had hired a person from ES&S to solve issues with the machines. Programming was the main reason for the problems, she said.
12	May 2006	Hart Intercivic eSlate	Texas	**Tarrant County, Texas.** Ballot programming error on the eSlate omits contests from the ballot.[41] Two City Council races were dropped from the Tarrant County ballot in areas of the city served by non-Arlington schools because of a voting machine programming oversight, county election officials said Monday.

[39] **NPR: Morning Edition,** 6 November 2002; "Analysis: Senate races in Minnesota and South Dakota" Referenced in *Black Box Voting* by Bev Harris, Chapter 2.

[40] **Vendor bender. City clerk blames ES&S for Election Day difficulties.** Times Record News. May 14, 2006. By Robert Morgan. http://www.votersunite.org/article.asp?id=6598

[41] **Ballot problems mark 1st day of early voting.** Star-Telegram. May 2, 2006. By Neil Strassman. http://www.dfw.com/mld/dfw/news/local/14479735.htm

Vote-Switching Software Provided by Vendors — A Partial List Reported in the News

Map#	Date	Machine	State	Place/Description
15	March 2006	ES&S Optical AIS 315	**Texas**	**Webb County, Texas** ES&S blamed by county for errors in programming and inadequately training county staff.[42] Due to a programming error, the PEBs could not be used and tabulators had to read each individual flash card, significantly delaying the vote tally. The company prepared all software for the election. Additional problems cited include delays of three days before receiving coding for electronic ballots, following mistakes involving receipt of nearby McMullen County codes. The County is considering a suit against ES&S.[43] Webb County Commissioners Court may take its first step toward suing Election Systems and Software, Inc. today. The county paid nearly $900,000 for the electronic voting machines that officials alleged had programming errors and inadequately trained staff.
20	March 2004	ES&S Optical Scan	**Texas**	**Lubbock County, Texas.**[44] The machines failed to count the votes for the Precinct 8 Democratic chairman race. Dorothy Kennedy, Lubbock County elections administrator said they would need to recount all the ballots for all races in the county. She said Omaha, Neb.-based ES&S, which prepared the vote tabulators, will foot the bill for the recount.

[42] **Election Uproar; County officials say there were plenty of red flags** Laredo Morning Times, March 14, 2006 by Julie Daffern. http://www.zwire.com/site/index.cfm?newsid=16299334&BRD=2290&PAG=461&dept_id=473478&rfi=8

[43] **Suit eyed in vote machine controversy.** Laredo Morning Times, June 12, 2006. By Kirsten Crow. http://www.lmtonline.com/site/news.cfm?newsid=16776354&BRD=2290&PAG=461&dept_id=569392&rfi=6

[44] **Software blamed in Precinct 8 Democratic chair race mixup.** Lubbock online.com; March 11, 2004; By Brian Williams, Avalanche-Journal http://www.lubbockonline.com/stories/031104/loc_031104030.shtml

Vote-Switching Software Provided by Vendors — A Partial List Reported in the News

Map#	Date	Machine	State	Place/Description
n/a	March 2004	Unity Election Management Software	Texas	**Bexar County, Texas.** Misprogramming causes the Unity software to balk at accumulating votes from the optical scan machines used to count absentee ballots. [45] Tabulation of the Bexar County votes was delayed for about 1 1/2 hours, beginning about 8 p.m. ..."They have big problems," said Nick Peña, a poll watcher for District 28 U.S. Rep. Ciro Rodriguez, D-San Antonio. "They look very worried. "They have a bunch of technicians in the tabulation room, and they are pulling out wires and reattaching them, and the computer screens are all frozen. You can tell that something is happening," Peña said. ... Borofsky said the delay occurred after it was discovered the tabulation computers hadn't been properly programmed with updated data in order to count the mail-in paper ballots. The computer system then was taken off line and updated with the information needed to process the 3,000 paper ballots, which were tabulated using high-speed scanners.
n/a	November 2002	ES&S optical scan	Texas	**Scurry County, Texas.** A landslide victory for two commissioner candidates caused poll workers to question the results. The chip in the ES&S 650 contained an incorrect ballot program. ES&S sent a new chip, and the county officials also counted the votes by hand. The opposing candidates actually won by large margins.[46]

[45] **Bexar computer glitch delays counting of votes.** San Antonio Express News. March 10, 2004. Tom Bower. http://www.mysanantonio.com/news/metro/stories/MYSA10.12A.VotingProblems0310.4ea013d9.html

[46] 06/03/04. Conversation with Scurry County Elections Director, who told VotersUnite it was an ES&S 650. She said it was the chip with the ballot programming on it, that they had to get a new one from ES&S. Original reference was from *Black Box Voting*, Chapter 2. Houston Chronicle, 8 November 2002; "Ballot glitches reverse two election results"

Vote-Switching Software Provided by Vendors — A Partial List Reported in the News

Map#	Date	Machine	State	Place/Description
n/a	April 2002	Optical Scan and iVotronic	Texas	**Dallas County, Texas.** A ballot programming error tallies 18 results incorrectly. Here is one case when flawed ballot data on a paperless electronic voting machine caused a serious election miscount. It was detected only because voters also used optical scan paper ballots in the election.[47] Mrs. Hawkins-Curtis, a candidate for Rowlett mayor was added to the ballot four days before the start of early voting. The change in the ballot definition wasn't programmed into all 390 ES&S iVotronic machines until after early voting began. The ballot data was changed only in Rowlett polling places. When the results were combined with the results from ES&S optical scan machines, the error caused the tally software to improperly tally results in the mayor's race as well as 17 other races, including propositions and school board races. Nearly 5,000 of the 18,000 ballots were improperly counted. An initial count didn't reveal a problem, and the results of all races were posted as final but "unofficial" on the Election Department's Web site at 10:17 p.m. Saturday. A few minutes later, a second count - called the reconciliation process - began to show that the number of voters who signed in at numerous precincts didn't match the vote totals, Ms. Pippins-Poole [county's assistant elections administrator] said. The extent of the miscount wasn't discovered until Monday when Election Systems & Software began a thorough investigation, Ms. Pippins-Poole said. ...The touch-screen ballots have been used in early voting in 91 elections since 1998 without any problems, Ms. Pippins-Poole said.

[47] **Glitch affects 18 races: Problems in counting early votes could alter some election outcomes.** Dallas Morning News. May 8, 2002. Ed Housewright, staff writer.

Vote-Switching Software Provided by Vendors — A Partial List Reported in the News

Map#	Date	Machine	State	Place/Description
n/a	November 1998	Votronic and Model 100	**Texas**	**Dallas, Texas** A software programming error caused Dallas County, Texas's new, $3.8 million high-tech ballot system to miss 41,015 votes during the November 1998 election. The system refused to count votes from 98 precincts, telling itself they had already been counted. Operators and election officials didn't realize they had a problem until after they'd released "final" totals that omitted nearly one in eight votes. The system vendor, ES&S, assured voters that votes were never lost, just uncounted. The company took responsibility and was trying to find two apparently unrelated software bugs, one that mistakenly indicated precinct votes were in when they weren't, and another that forgot to include 8,400 mail-in ballots in the final tally. Democrats were livid and suspicious, but Tom Eschberger of ES&S said, "What we had was a speed bump along the way."[48] After Nov. 3, Sherbet was quoted in the Dallas Morning News as saying, "In 17 years of doing this, there's been nothing more troublesome to me, more humiliating."[49]
6	May 2006	ES&S Optical Scanners	**West Virginia**	**Taylor County, Upshur County, and Mineral County, West Virginia.** ES&S provided flawed programming for the optical scanners. [50] None of Taylor County's votes could be counted last night because the main computer would not read tabulators from individual voting machines. Upshur County's counter was in such bad shape that as of midnight the county was trying to get a similar machine from a neighboring county. Mineral County's optical scan ballot counter was producing **skewed results.**
7	May 2006	ES&S Optical Scanners	**West Virginia**	**Kanawha County, West Virginia.** Ballot programming flaws were provided by ES&S.[51] Kanawha County officials tried to test the county's new optical scan voting machines on Tuesday, but were unable to complete the dry run because the machines were not fully programmed.

[48] **Black Box Voting** by Bev Harris, Chapter 2.

[49] **Who Counts The Votes?** By Gary Ashwill and Chris Kromm. http://www.southernstudies.org/reports/votingmachines-new.htm

[50] **Several Counties Have Vote Counting Problems. New voting systems were used for the first time.** WOWKTV 13. May 10, 2006. by Dave Kirby. http://wowktv.com/story.cfm?func=viewstory&storyid=10787

[51] **Kanawha's dry run of voting machines remains incomplete.** Charleston Gazette. May 03, 2006. Archived at http://www.votersunite.org/article.asp?id=6596

Vote-Switching Software Provided by Vendors — A Partial List Reported in the News

Map#	Date	Machine	State	Place/Description
8	May 2006	ES&S iVotronic	**West Virginia**	**West Virginia.** ES&S ballot programming errors were discovered before the elections on iVotronics touch screens in 13 out of 34 counties using the machines.[52] Ireland said the number of counties reporting problems with ES&S-prepared ballot software has increased to 13 of the 34 counties that have contracts with the company to provide electronic voting systems. A glitch in some of the systems allows users of the company's Ivotronic [sic] machines to cast ballots and have their votes recorded correctly, but does not count the votes properly.
16	November 2004	ES&S Optical scan	**Wisconsin**	**Taylor County, Wisconsin (Medford).** Four and a half months after the election, a consulting firm discovered that ES&S had programmed the optical scanners incorrectly, failing to account for partisan elections. All straight-party votes were lost, affecting approximately 27% of the ballots.[53] That failure meant that the votes of everyone who voted straight ticket - anyone who voted only for candidates of a single party - were not counted. In all, about 600 of 2,256 ballots cast were not counted, [Taylor County Clerk Bruce] Strama said. ... Medford and Taylor County officials have been told by Nebraska-based Election Systems & Software that the city will be reimbursed for the costs of setting up the vote-counting machine in the fall because the program was faulty. A spokeswoman said the company takes full responsibility for the error. ... "There's really nothing voters can do at this point," said Kevin Kennedy, the executive secretary of the State Elections Board.

[52] **Election test delayed.** TMCnet. May 1, 2006. by Charleston Gazette staff writer Phil Kabler and The Associated Press. http://www.tmcnet.com/usubmit/2006/05/01/1628275.htm

[53] **About 600 Medford ballots cast in November ignored.** Marshfield News-Herald. March 12, 2004. By Jake Rigdon. http://www.wisinfo.com/newsherald/mnhlocal/285285292773470.shtml

Vote-Switching Software Provided by Vendors — A Partial List Reported in the News

Map#	Date	Machine	State	Place/Description
18	August 2004	ES&S Unity Election Management System	Wyoming	**Natrona County, Wyoming.** The Unity Election Management System, used to tally votes from both optical scan machines and paperless electronic voting machines, failed to tally votes correctly. [54] Noticing that the totals for the city of Evansville seemed low, Natrona County Clerk Mary Ann Collins checked the printouts from the precinct voting machines in Evansville and found that the totals didn't match the totals computed by the Unity software, which combines all the totals countywide. The error changes the order in which some candidates finished, but does not affect which candidates will advance to the general election. Only one candidate lost votes but five of the 10 municipal races in the county had changed totals. ... Collins determined the software problem only affected nonpartisan races after checking the voting machine printouts and the absentee votes against the Unity software report in several partisan races. There does not appear to be any pattern in the skewed vote totals.

[54] **Clerk changes election vote totals.** August 21, 2004. By Matthew Van Dusen, Star-Tribune staff writer.
http://www.casperstartribune.net/articles/2004/08/21/news/casper/6c2e825b3f9e154187256ef70007adbb.txt

Responses to:
Representative Holt's Additional Questions for Witnesses
Committee on House Administration Hearing on
Electronic Voting Machines: Verification, Security, and Paper Trails
September 28, 2006

(1) My legislation has 219 cosponsors today, largely due to the lobbying efforts of voters and concerned citizens. It is truly an example of democracy in action.

Could you share with the Committee your experience in working with the League of Women voters on this issue – as the League too experienced a "change of heart" also almost entirely due to a "democratic uprising" of the Members?

The League's early support for paperless Direct Recording Electronic (DRE) machines was troublesome for many League members, especially since the vulnerabilities of computers to hacking and insider manipulation are widely known. Perhaps even more disturbing was that the League's position was being used as a justification for the widespread purchase of paperless DREs.

How could this have happened? The great respect in which the League is held stems in large part from the care that the League traditionally has displayed in understanding and analyzing issues. The League studies an issue carefully before taking a position. Once a position is taken, the board determines what action, if any, to take as a result. While studies increase the time required to reach a position, careful examination combined with the consensus process protect the League from errors in judgment that might have serious repercussions.

Regrettably, the League did not conduct any study on electronic voting machines, nor did it consult with the membership. The national board decided to support paperless DREs based on their interpretation of the League's broadly written position on voting rights. The League leadership appeared to have relied on the advice of a couple of computer scientists, including Michael Shamos – who was quoted in several League documents and who spoke at the 2004 national League convention.

As a computer scientist who had been involved with voting issues for several years, I attempted to explain the risks of paperless DREs to the League lobbyists. While my efforts were unsuccessful, I was hardly alone among League members in feeling that the League had taken an unwise position. Leaguers from around the country asked the Board to discontinue its support of paperless DREs. Individual members wrote to President Kay Maxwell. Some Leagues, including the Massachusetts LWV[i], requested a change in the national position. A letter to President Maxwell, expressing concern about "National's stand against individual paper confirmation for each ballot (VVPAT)," was signed by 924 League members from 35 states. A similar letter was signed by twenty-two local and area Leagues from eight states.[ii]

At the 2004 national League convention, the delegates voted overwhelmingly for a new resolution calling for "the implementation of voting systems and procedures that are Secure, Accurate, Recountable, and Accessible". This is known as the SARA resolution. After the 2004 convention many members were surprised by the LWVUS leadership's misinterpretation of the SARA Resolution[iii]. The leadership claimed that SARA did not prevent the League from supporting paperless DREs. While the national League no longer endorsed paperless DREs, the leadership nonetheless signaled that they still approved of these machines, in part by allowing state and local Leagues to continue endorsing paperless DREs and by criticizing those Leagues that were advocating for voter verified paper ballots and random audits.

In a discussion of the Voter-Verifiable Paper Trail in *Helping America Vote*, a League document released a few days after the 2004 Convention[iv], Georgia and Maryland – two states using paperless DREs[v] – were credited as having best practices. In addition, the following sentence appears:

> "However, a paper trail is not the only means available for auditing the voting process."

Helping America Vote was undoubtedly written prior to the Convention[vi]. However, our expectation that the LWVUS leadership would subsequently embrace all of the SARA Resolution was dashed when President Kay Maxwell testified before the Commission on Federal Election Reform on April 18, 2005.

> The League of Women Voters believes that voting technologies must be secure, accurate, recountable, and accessible. The term "recountable" is not a code word for paper trail; indeed, the League's stand is based on the understanding that continued technological innovation is needed.

No one questions that continued technological innovation is needed. But we ignore at our peril the serious vulnerabilities of the voting machines being deployed in our elections now. Furthermore, the SARA resolution did not equivocate on the meaning of the word "recountable".

The notion that "recountable is not a code word for paper" was repeated on other occasions by League leadership[vii].

I have asked League members and others who claim that paperless DREs can be recounted to explain precisely how to conduct such a recount, for example in cases such as Carteret County, NC where over 4000 votes were lost on a paperless DRE in the 2004 election[viii]. I have never received a satisfactory answer. Of course one can always print out the contents of the computer's memory and count that. But that is a reprint, not a recount.

In the dramatic 2004 recount for Governor of Washington State, the Secretary of State and the political parties implicitly acknowledged the impossibility of a meaningful

recount of paperless DREs. They all agreed not to print out copies of ballots from paperless DREs. Instead, they simply compared earlier results with recomputed ones.[ix]

Because of the League leadership's stance on what "recountable" meant, or did not mean, those members who had worked very hard for the passage of the SARA Resolution realized that they had more work to do. Since the League holds its national convention every two years, the next opportunity to clarify the League's position did not come until June 2006. In order to make sure that there would be no further confusion, a large majority at the 2006 convention passed the following resolution:

Whereas: Some LWVs have had difficulty applying the SARA Resolution (Secure, Accurate, Recountable and Accessible) passed at the last Convention, and
Whereas: Paperless electronic voting systems are not inherently secure, can malfunction, and do not provide a recountable audit trail,
Therefore be it resolved that:

> The position on the Citizens' Right to Vote be interpreted to affirm that LWVUS supports only voting systems that are designed so that:
>
> 1. they employ a voter-verifiable paper ballot or other paper record, said paper being the official record of the voter's intent; and
> 2. the voter can verify, either by eye or with the aid of suitable devices for those who have impaired vision, that the paper ballot/record accurately reflects his or her intent; and
> 3. such verification takes place while the voter is still in the process of voting; and
> 4. the paper ballot/record is used for audits and recounts; and
> 5. the vote totals can be verified by an independent hand count of the paper ballot/record; and
> 6. routine audits of the paper ballot/record in randomly selected precincts can be conducted in every election, and the results published by the jurisdiction.

The central theme of the League of Women Voters, and of the suffrage movement on which it was founded, is that every citizen should have the right to vote and to have that vote accurately counted. The work of the members who brought the two SARA resolutions to the League Conventions, combined with the overwhelming approval of those resolutions, are in the best tradition of the League.

Active support by the League for voter verifiable paper ballots combined with mandatory random manual audits for all elections will be a major contribution to the increased security and accountability of our elections.

Few things are more important to our democracy.

(2) Michael Shamos opened his testimony by stating the following – "[t]he proposed bill is based on three major assumptions, all of which are false. First, it assumes that paper records are more secure than electronic ones, a proposition that has repeatedly been shown to be wrong throughout history. Second, it assumes that voting machines without

voter-verified paper trails are unauditable because they are claimed to be "paperless," which is also false. They are neither paperless nor unauditable. Third, it assumes that paper trails actually solve the problems exhibited by DRE machines, which is likewise incorrect." Do you agree with Mr. Shamos' analysis, and if not, why not?

I do not agree with Mr. Shamos claims, and I do not understand why he continues to make these claims in the face of overwhelming evidence to the contrary.

First, it assumes that paper records are more secure than electronic ones, a proposition that has repeatedly been shown to be wrong throughout history.

Security is an issue with any type of voting records.

There is much more history with elections using paper records than with electronic records. It is well understood how to minimize the security risks in an election using paper records by having the transport and the counting of the ballots observed by representatives of the major parties. However, there is no satisfactory way for an observer of a purely electronic election to satisfy himself or herself that the count was done correctly and honestly.

Mr. Shamos has stated that there has not been a verified instance of election tampering using paperless DREs. However, Mr. Shamos is unable to guarantee that no one has ever exploited the security holes that have been uncovered by computer security experts like Felten, Hursti, and Rubin. Mr. Shamos cannot make that guarantee because no one can. It is not possible, given the way we run elections, to verify that an election held on paperless DREs has not been subverted by malicious code.

The report from Cuyahuga County[x], cited in Mr Shamos' testimony, reveals problems with both the electronic and the paper ballots. There were massive failures of every sort, including touchscreens freezing, voter access cards sticking, DRE legs breaking, and other unfamiliar and unexpected events[xi]. Many of these failures can be attributed to the really poor engineering of the DRE and the sloppy retrofits that were made for the VVPAT, as well as inadequate training, policies, and procedures.

But perhaps the most significant findings of the Cuyahoga County report were the problems associated with the memory cards that contain the vote records. For example, twelve memory cards were lost[xii] and four memory cards were found in DREs several weeks after the election[xiii]. Consequently, some of the reports findings are:[xiv]

> **Information on DRE memory cards can be automatically deleted.**
>
> **The memory cards used for electronic voting in Cuyahoga County have a potential for tampering, excessive expense, and chain of custody concerns.** [emphasis in original]

The report also makes clear that the VVPAT used in Cuyahoga County was poorly engineered and had poor usability and human factors.[xv] Furthermore, because poll workers were inadequately trained and the public insufficiently informed, "Some voters were unaware that they could lift the blue covering of the printer to observe the print out and verify their vote"[xvi]. Many of the paper jams would undoubtedly have been spotted a lot earlier had the opaque cover been opened, instead of left closed.

Consequently, the lessons from Cuyahoga County do not support Mr. Shamos' claim. There were severe problems with both the memory cards and the VVPAT. Furthermore, the VVPAT implementation was far from the state-of-the-art in paper ballot systems.

Second, it assumes that voting machines without voter-verified paper trails are unauditable because they are claimed to be "paperless," which is also false.

No practical alternative means of auditing an election has been proposed. Any alternative auditing method would have to have the utmost confidence of the general public. There is no reason for people to trust the numbers printed out by a DRE at the end of the Election Day, as Professor Felten has demonstrated.

Mr. Shamos stated in his written testimony[xvii]:

> Numerous effective verification methods are known that are not based on vulnerable paper records. These have not yet been implemented in viable commercial systems. I understand that scientists at NIST will soon announce another one.

The only reference to any specific proposal provided by Mr. Shamos was to a new scheme by Prof. Ronald Rivest of MIT. Since this scheme is paper based, it is not a paperless method of auditing.

In his oral testimony Mr. Shamos also suggested an approach involving two screens and a video camera in his oral testimony. In addition to being totally impractical, the video camera approach raises major problems involving privacy and the difficulty of conducting an audit or a recount.

Third, it assumes that paper trails actually solve the problems exhibited by DRE machines, which is likewise incorrect.

This claim appears to be based on recent experiences with DREs that have been retrofitted with poorly engineered VVPATs. Mr. Shamos seems to have overlooked the existence of optical scan based systems that produce easily audited Voter Verified Paper Ballots.

The best voting system currently available for voters without vision or mobility problems is the precinct based optical scan system. Proponents of DREs argue that optical scan systems are not accessible. As I discussed in my testimony, there are devices, such as the

Vote-PAD, that allow blind, and even blind-deaf voters (who cannot vote unassisted on DREs), to vote independently on optical scan ballots and to verify those ballots.

The AutoMARK and the Populex electronic voting system also produce accessible Voter Verified Paper Ballots that can be tabulated by an optical scanner. Because neither system records or counts votes internally, they are not subject to the kind of vote rigging that has been demonstrated for DREs. However, for all of these systems it is crucial that a random manual audit be conducted in all elections as a check on the accuracy of optical scanners.

Some of the retrofits done to paperless DREs by adding continuous roll thermal printed paper are poorly engineered. However, these retrofits are far superior to paperless DREs. At least with the retrofitted machines there is a chance that an effective audit or recount might be conducted. There is no technical reason why DREs with VVPATs that use reliable printer technology combined with good usability could not be produced.

(3) In your testimony you described a report by Kelly Pierce, a nationally-known advocate for the blind and visually impaired, who had reviewed four voting machines in March, 2005 for the Cook County Ohio State's Attorney's Office. In his report, entitled, Accessibility Analysis of Four Proposed Voting Machines, you indicated that Mr. Pierce "analyzed tactually discernable controls, spoken prompts, visual display, poll worker assistance, volume control and normalization, and ballot review" and "found all four machines deficient in one or another of these areas. . ." You quoted Mr. Pierce as saying "[u]nfortunately," if any one of the four machines were to be deployed in Chicago or suburban Cook County as exhibited on March 15, many voters with disabilities, particularly blind voters, would not be able to cast a ballot independently and privately". Mr. Dickson took exception to your testimony on this subject, suggesting that all of the problems pointed out in the Pierce study had since been corrected. Do you agree, and if not, why not?

No one, including Mr. Dickson, is claiming that all of the accessibility problems identified in Mr. Pierce's report have been eliminated from new models of all DREs, let alone from the installed base of voting machines already in the field. Indeed, a serious question that is not being addressed is just who would pay for upgrades to repair machines that are defective from both a security *and* an accessibility standpoint. The situation in Cook County is atypical, because Cook County has a population and purchasing power greater than some states. As the Chicago Tribune noted,[xviii] Chicago and Cook County are "... Sequoia's biggest piece of business in the nation." Most counties do not find the manufacturers, even Sequoia, as cooperative as Mr. Pierce has found Sequoia to be with his county.

Mr. Pierce's report, while a highly worthwhile and useful document, was written primarily from the perspective of a totally blind voter. It does not, for example, deal much with issues such as lack of voter adjustable controls for color, contrast, and magnification, nor with physical access to the machines for voters who use wheelchairs.

It discusses neither 2-switch input controls nor issues for voters who are deaf/blind for whom DREs are totally inaccessible. Mr. Pierce's report is generally silent on accessibility issues for voters who have learning or cognitive disabilities.

Additional problems with the Sequoia machines used for the March 21, 2006 primaries were uncovered in a report released in April 2006 by the Illinois Ballot Integrity Project.[xix] On page 15 of the Ballot Integrity Project report presented to the Cook County Board of Commissioners, we find:

> For example, the SBOE [State Board of Elections] staff tested the audio interface, but apparently no testing was done with any other assistive devices for which the AVC Edge might be equipped, such as sip-puff. While the sip-puff feature which allows access for severely physically disabled voters has been made available in other jurisdictions, it was not tested in Illinois, nor were the AVC Edge DREs used in Chicago and Cook County during Early Voting and on March 21, 2006, so equipped.

The report continues with the following on page 16:

> One final consideration with respect to Section 301(a)(3) compliance requires mentioning and that is accessibility for those voters who require wheelchairs. Although the AVC Edge design incorporates a "wide-leg" design, almost all voters using wheelchairs are unable to reach the top displays on the touchscreen. While theoretically, one might consider using the keypad provided for non-sighted voters, this option is precluded because once the keypad is connected, the screen goes blank. Therefore, those sighted voters using wheelchairs would be forced to use the audio-prompt system which requires a substantially greater amount of time and would be both inconvenient and confusing.
>
> We have provided a significant commentary on the Section 301(a) compliance features of the AVC Edge because it's this aspect that provides voting machine manufacturers and election officials with the strongest rationale for selling and purchasing these machines. Approximately $21 million are to be spent by the City and County for the purchase of DRE equipment. We must ask, was that equipment properly tested and certified by the State Board of Elections for the primary purpose for which it was intended? The absence of such testing and the SBOE (or the City or County) failing to require sip-puff features suggest that it was not. One might even speculate that actual compliance was less on the mind of the Illinois State Board of Elections than placing responsibility for compliance elsewhere:
>
> > "I want somebody to say today they're taking that responsibility [for disabled accessibility] and that it's not ours, because I don't want us being liable and that [disabled] community, you know, blaming us for allowing this to be out there. And you know, as I said, I'm just wanting to protect this Board from some things that we can't necessarily control that you [Sequoia] will be."[xx]

Later on page 16 there is the following:

> Despite two out of five DREs experiencing paper jams, significant shortcomings in the audio-assist component raised by both the disabled community and its own Director of Voting Systems Standards, having had no reference to the ITA report, non-compliance with Section 301(a)(3) and questions about compliance with Section 24C-2 of the Illinois Election Code, the Board granted interim certification to the "Sequoia AVC Edge Product" by unanimous vote. Due diligence or rush to judgment?

Possibly even more relevant to our discussion, neither the Pierce report nor his recent letter, dated October 4, 2006 (see below), addresses the issue of accessible voter verified paper audit trails, an issue that is of concern to many voters with disabilities. In addition to Natalie Wormeli's eloquent testimony included in my written statement, see for example:

- *A Verifiable, Accessible Vote*, October 11, 2004 letter to the New York Times from Barbara Silverstone, Chief Executive, Lighthouse International[xxi]
- *Touch Screens are not the best Choice for Disabled Voters*, by A. J. Devies, President, Handicapped Adults of Volusia County[xxii]
- The list of at least seven organizations representing New York State voters with disabilities[xxiii] who signed The New York State Citizen's Coalition on HAVA Implementation. A key point of the Coalitions platform is the following: *New voting machines should provide a "voter-verifiable paper audit trail" and incorporate "data-to-voice" technology to ensure full access by all.*[xxiv]

Mr. Pierce analyzed four voting machines in his initial report dated March 23, 2005: the iVotronic from Election Systems and Software, the AVC Edge II from Sequoia Voting Systems, the eSlate from Hart InterCivic, and the AccuVote TS from Global Diebold. I referenced this report in both my written and oral testimony. In his oral comment, Mr. Dickson said:

> The rest of the story is that after those initial texts ***the company*** [emphasis added] was able to inexpensively and quickly make changes to the access procedures so that the problems were eliminated.[xxv]

It remains unclear to me as to why Mr. Dickson rose to the defense of *one* voting machine vendor in these Congressional hearings, when I clearly had just referenced a report that surveyed *four* voting machine vendors. He did not name the vendor to which he was referring, nor did he say why he defended one vendor from among the four that were cited. His comment gave the appearance, however, of suggesting that the problems of all of the vendors had been fixed.

While Mr. Dickson chose not to address the accessibility of all four of the voting systems analyzed in the Pierce report, voting machine access problems have hardly been eliminated, as I discuss below.

It was only after the hearing that I learned that Mr. Pierce, in response to my testimony, was preparing his October 4, 2006 update letter.[xxvi] However, the letter, included with this response, appears to update a report he wrote for the Cook County State's Attorney's Office dated June 30, 2005, entitled *Evaluation of Audio Interface Sequoia Voting Systems AVC Edge*. It is not an update to Mr. Pierce's earlier March 23, 2005 report, referenced in my testimony.

In his letter, Mr. Pierce does not mention the four voting machines he analyzed in 2005. Instead, he refers only to the Sequoia Edge II Plus voting system that is scheduled to replace the Sequoia AVC Edge II, used in the March primary, for the November 2006 election in Cook County. While Mr. Pierce's comments appear to suggest that the Edge II problems have also been fixed, it does not appear that Sequoia changed its access procedures for the Edge II. They did, however, make changes to the scripts of the messages.

The Sequoia Edge II Plus does not represent simply a minor change in the features and software of the Edge II. Rather, it is based on the Smartmatic voting system used in Venezuela. Smartmatic International, a Venezuela based company, is the parent company of Sequoia Voting Systems[xxvii].

Like Mr. Dickson, Mr. Pierce's update letter makes no reference to the other three flawed voting systems. In the interest of furthering improvement to the accessibility of voting systems for people with disabilities, we first discuss the four voting machines analyzed in Pierce's original report.

According to Noel Runyan, the blind computer scientist and accessibility engineer quoted by Mr. Pierce in his original report, the following accessibility problems, originally identified by Mr. Pierce, do not appear to have been fixed on currently shipping systems[xxviii]. All italicized text describing unfixed problems in the four voting machines are direct quotes from *Accessibility Analysis of Four Proposed Voting Machines*, by Kelly Pierce, Cook County State's Attorney's Office, March 23, 2005.

Accuvote TS from Diebold:

- The selection of access options must be done for the voter by a poll worker.
- The keypad cannot be operated with a closed fist.
- There still *is no prompting of end users asking them if they want the screen turned off* or giving them a control to do so independently.

Edge II from Sequoia:

- The machine does not have simultaneous audio and visual output.
- The keypad does not permit operation with one hand or closed fist.
- The language selection menu still has requirement for pressing Select twice to exit.
- There still is the time-out bug that pops you back into the language menu.
- The audio ballot review is still a non-pausable long drink from a fire hose.
- *The voting machine from Sequoia functioned poorly at ballot review.*

- *The opening of contests and single and double button pushes adds to the complexity of the machine.*
- *After pressing a button, the Sequoia machine immediately advanced to the next contest with no information about what one exactly voted for and the ability to change one's vote in the event of error.*

eSlate from Hart:

- The keys are still not tactilly discernable.
- The navigation wheel is still too small, requiring fine motor control that is hard or impossible to do with a closed fist, mouth stick, etc.
- The machine does not have built-in volume control and does not reset to normal value for each new voter.
- *The only machine showing difficulty producing adequate volume was the eSlate by Hart InterCivic.*
- *The Hart InterCivic machine had more systemic issues with missing scripts, omitted information about the location of controls and a lack of prompting after a voter had voted in a contest so the voter knew what to do next to advance to the next race.*
- *Unfortunately, when end users change their votes in ballot review, they are left in the original voting screen and need to scroll all the way to the bottom of the ballot to exit.*

iVotronic from ES&S:

- The machine does not have simultaneous audio and visual output.
- The machine does not have built-in volume control and does not reset to normal value for each new voter.
- The selection of the audio output feature must be done for the voter by poll worker.
- There is no audio rate control.
- *By contrast, the IVotronic from ES&S would likely need much more script revision to ensure full understanding and clarity of the interface. In addition, new audio prompts would need to be added to help users of the audio ballot take the next step in progressing through the ballot.*
- *For example, after the end user has cast a vote in a particular contest, the system confirms the vote but it fails to instruct the end user as how to use the machine to advance to the next contest and cast a vote in that contest.*

Many of the problems cited in Pierce's original report remain in the Edge II Plus system discussed in his update letter. Again, quoting from Noel Runyan about the Sequoia Edge II Plus system[xxix]:

- There is no simultaneous audio/video on the current Edge II and none on the Edge II Plus planned for use in this November 2006 election.
- The 2-switch feature, while better than none, is a Band-Aid on a Band-Aid. For the Edge II, it does not include any change in the orientation and help messages to aid in the proper use of the 2-switch controls. The Edge II also currently requires

that 2-switch users and other keypad users get their output in audio, without any video display, as if they were also blind.
- The new V5 keypad for Edge II systems does not support one-handed use and both it and the newer keypad that is supposed to be available on the Edge II Plus systems are still not operable with a closed fist.

The Edge II on which Mr. Runyan voted in the California June primary contained the newer software for the Edge II system. Nonetheless, Mr. Runyan still encountered major problems. Workers had great difficulty in setting up the Sequoia Edge II machines in proper audio mode. Bugs, such as the time-out bounce back to the language menu, also remained unfixed.

At this point it is nearly impossible to know just which accessibility problems on the Sequoia Edge II have been fixed in the Edge II Plus and how effective those fixes may be, because – unfortunately – neither the specifications for the Edge II Plus nor the results of usability and accessibility tests are publicly available. However, experience has shown that it is unwise to accept vendors' fixes and promises until the results can be demonstrated in real, certified, delivered machines. It appears that proper access usability testing has not been done on the Edge Two Plus systems in Illinois or elsewhere.

Regarding the cost of upgrading existing machines, Mr. Runyan makes the following observations[xxx]:

> Another relevant issue is the cost of upgrading existing voting systems to take advantage of any of these changes – where possible. Some activists have been saying that we should go ahead and rush into buying the current DRE machines, despite their known security and access flaws, and then we can count on them being fixed or improved in the future. Even if the major problems could ever be solved, what will be the price and who will pay it? Certainly, not the Manufacturers.
>
> According to our local ROV office, Sequoia normally asks roughly $250 each to upgrade Edge II systems to the V5 keypads that have rate control keys and a jack for 2-switch input controls.
>
> According to reports in January, the state of New Mexico was about to pay around $16 million to upgrade their mostly Sequoia Advantage voting systems to Sequoia systems that could have VVPAT paper trails. Additionally, the NM Secretary of State was going to do in December 2005, as some activists would have us do – buy more of the same flawed and obsolete systems ($5 million more for NM).
>
> As a blind voter, I am impatient with the slow pace of adoption of secure and accessible voting systems. However, I feel strongly that it is extremely irresponsible for counties to rush into buying more flawed voting systems. To be specific about the VVPAT issue, I believe that, given the current voting systems designs, no new voting systems should be purchased unless they have accessible voter verifiable and auditable paper record capability such as is already available

with at least one of the ballot marking systems.

I also feel that the best way to solve the accessibility, usability, and security problems is to stop piling band aids on the old, obsolete DRE systems and introduce completely new voting systems whose designs included security and accessibility/usability considerations from the beginning of their conception. To meet the flexible accommodation requirements for usability and accessibility by a diverse population of voters, the current and future systems will need to employ modular systems and/or blends of various voting machines.

(4) Since 1990 (and as set forth in the current EAC Voluntary Voting System Guidelines), federal voting machine standards have specified a mean time between failures (MTBF) of 163 hours. This corresponds to a nearly 10% probability of machine failure on Election Day. Current machines appear to perform no better than the standards require. Modern technology is fully capable of MTBF's in the range of 15000 hours. What are your thoughts on the impact this reliability standard is having on the accuracy of our election process?

It is easy to see how unconscionably weak the voting system MTBF standard is by comparing it with the MTBF for devices in common use today. For example, according to a study by Compaq Corp, a thin client PC, which in many ways resembles a DRE, typically has a MTBF of up to 170,000 hours[xxxi], as opposed to 163 hours. Nonetheless, the 163-hour MTBF standard was included in both the 2002 Voting System Standards/Guidelines[xxxii] and the recent 2005 Voluntary Voting System Guidelines[xxxiii].

Another disturbing aspect of the current MTBF standard is that "failure" can mean just about anything, including problems that are obvious to the voter, e.g. screen failure, and those that are hidden from the voter, e.g. failure to accurately record an individual's vote. For example, 4,438 votes were irretrievably lost in early voting on paperless DREs in Carteret County, North Carolina in 2004. After recording about 3000 votes, the machine simply stopped recording votes[xxxiv].

High DRE failure rates combined with the lack of back-up paper ballots will disenfranchise voters, since most people are unable to spend hours waiting in line in order to cast their votes.

Because voters dependent on DREs are more likely to be unable to vote than voters using optical scan or ballot marking voting systems, the use of unreliable DREs with no paper ballot voting options is an Equal Protection issue[xxxv].

DRE failures also impact disabled voters disproportionately by making it not possible for those voters to vote privately or independently.

The impact of deploying unreliable voting machines that have no paper trail can be severe. For instance, according to the Montgomery County (Maryland) Board of

Elections in a report entitled, *2004 Presidential General Election Review, Lessons Learned*[xxxvi]:

> From Help Desk tickets and [Diebold] GEMS reports, 189 voting units (7%) of units deployed failed on Election Day. An additional 122 voting units (or 5%) were suspect based on number of votes captured.

As a result of the large number of failures, additional tests were conducted on failed voting units. One of the unfortunate Lessons Learned by Montgomery County was that in future elections they would need even more voting machines than they had anticipated.

> At noon today (Dec. 13, 2004), 148 voting units have been tested; of these, 35 have failed. Failed voting units will be returned to Diebold for further testing and repair or replacement. BOE has requested that Diebold formulate and provide us with a testing methodology and capture all results and subsequent repairs. Recommend: *For future elections, deploy more voting units on Election Day, beyond the allotted one unit for every 200 voters to offset the higher than expected failure rate.* [Emphasis added]

The requirement that machines have redundant memories gives no protection if the failure is some kind of "common mode" failure that affects both memories. In that case, the lost votes would be irretrievable. An example of a common mode failure is an electrostatic discharge (ESD) into the electronics that feeds data to the memories[xxxvii]. In spite of the fact that touch screen technology is highly vulnerable to ESD, the machines are tested to less than half the voltage that can be expected in a carpeted polling place on a day with relative humidity under 25%. In addition, the practice of removing memories at poll closing for vote tabulation is dangerous. The IEEE P1583 draft voting machine standards that was provided to the NIST/EAC process had an added provision requiring additional testing if devices are removed during poll closing. Unfortunately, that provision never made it to the VVSG. ESD is highly dependent on relative humidity, if the people accessing the electronics are properly grounded (such as if they are wearing grounding straps – advised in manuals for most electronic equipment and mandatory for access to the internals of military electronics) and the materials in clothing, chair coverings, and floor coverings[xxxviii].

As Michael Shamos is quoted as saying in a December 2005 article[xxxix], we should be in an uproar about the failure rate of DREs:

> "I have good reason to believe that 10 percent of systems are failing on Election Day. That's an unbelievable number," Shamos told an assemblage of voting-system makers, elections officials and scientists. "Why are we not in an uproar about the failure of (touch-screen voting) systems?"

This is the letter sent by Kelly Pierce that is referenced in my response to question 3.

OFFICE OF THE STATE'S ATTORNEY
COOK COUNTY, ILLINOIS

RICHARD A. DEVINE
Interest Bureau
STATE'S ATTORNEY
Washington - Suite 930

Chicago, IL 60602

Public

69 W.

312-603-8600

To: Interested Persons

From: Kelly Pierce, Disability Specialist

Date: October 4, 2006

I have become aware of widespread citation of my March 2005 accessibility review of four voting machines that were being considered for purchase by Cook County and the City of Chicago Board of Election Commissioners. Since this report was written, meaningful and substantial accessibility improvements have occurred. Following the public demonstration of the four voting machines on March 15, 2005, Cook County Clerk David Orr announced on May 26, 2005 that he had chosen Sequoia Voting Systems as the new election system for suburban Cook County. The next week, the Chicago Board of Elections followed with a similar announcement. The first electronic voting machine to be used would be the AVC Edge. On June 13, 2005, Sequoia Voting Systems then President and CEO Tracey Graham met with disability leaders and the Cook County Clerk and described the company's substantial commitment to improving the accessibility of the AVC Edge. An audio recording of a voting experience was produced that day following this meeting. The recording and end user experiences with the Sequoia AVC Edge were used to produce a June 30, 2005 report on the audio interface of the machine. Since completion of the report, Sequoia representatives spent more than 100 hours in enhancing and improving the audio script used by the AVC Edge, states a December 2005 memorandum by Sequoia President Jack Blaine. More than 20 hours were spent with city and county officials and leaders from the disability community reviewing the effectiveness of each audio prompt on the machine. Further, Sequoia redesigned its control box for the audio interface. The new control unit included easy to locate volume control buttons and a switch that increased or decreased the rate of speech in the audio recording. The new control unit also enabled those who could not use their hands to vote to plug in a sip and puff device so the ballot could be voted completely from someone's assistive technology.

Additionally, Sequoia committed to numerous other changes for the November 2006 election. In September 2006, Sequoia representatives met with the Cook County Clerk, the Executive Director of the Chicago Board of Election Commissioners and leaders in the disability community to demonstrate the new and enhanced accessibility features of the Sequoia Edge II Plus voting machine, which will be used in the November 2006 election. The Sequoia Edge II Plus replaces the AVC Edge used in the March primary election. The audio interface now includes navigational prompts on the contest menu and an interactive ballot review mode so blind and disabled voters can exit the review mode at a particular contest and change their selection as sighted voters can. The now accessible ballot review will largely resolve the problems

that were described in my report by a Santa Clara County, California blind voter. The experiences of this voter, which were quoted in the report, were shared recently in testimony before a congressional committee. The company may refine the accessibility of its ballot review, further increasing the accessibility and usability of this newly accessible function. The re-designed touch screen on the Edge II Plus has legs that can be adjusted to different levels for various wheelchair heights. For the first time, people who have low vision will be able to view the ballot using a zoom function which magnifies the type up to 400 percent its normal size as well as view the ballot at a high color contrast. Sequoia has re-designed its audio control unit yet again. The buttons are concave and recessed so those with head or mouth sticks and pointing devices can operate the machine independently. There are now also separate large plug-in "buddy buttons" for people with limited dexterity to use. More substantial enhancements to the accessibility of the Sequoia Edge II Plus are planned in time for the municipal elections in spring 2007.

At that time, most, if not all, of the accessibility problems identified in March 2006 will be dramatically reduced if not eliminated altogether. The flexible nature of information technology as deployed as electronic voting machines made the accessibility changes and enhancements possible. As has been stated in multiple reports by the National Council on Disability, a federal agency, when representatives of industry, government, and the disability community work together cooperatively as partners in using technology to solve accessibility problems, the inconceivable becomes possible enabling a new level of independence never before achieved.

---

[i] Letter to President Kay Maxwell from Madhu J. Sridhar, President, Massachusetts LWV, dated March 25, 2004.

[ii] Both letters and the list of signers can be found at http://www.leagueissues.org.

[iii] So far as I know, the LWVUS never posted the SARA resolution on the publicly accessible portion of the website. I also have been unable to find it on the member only portion, but my guess is that it's buried somewhere on the website.

[iv] *Helping America Vote*, written by Tracy Warren in collaboration with Lloyd Leonard, Jeanette Senecal, and Kelly Ceballos, 2004.

[v] They both use Diebold TS paperless DREs, the machine that Prof. Ed Felten has demonstrated to be highly vulnerable to election fraud.

[vi] But the leadership knew that a voting machine resolution was going to be introduced and might pass.

[vii] For example, on page 12 of the October 2004 issue of *The National Voter* (the publication sent to all LWV members), the SARA resolution is followed by the following sentence. "Since these criteria are not code words for any particular voting technology, the League neither supports nor opposes any type of technology per se, such as Direct Recording Electronic Voting Machines (DREs), Voter Verified Paper Trails (VVPTs) or optical scan".

[viii] *Making Votes Count: One Last Election Result*, New York Times editorial, January 18, 2004, http://www.nytimes.com/2005/01/18/opinion/18tues1.html?ex=1107100499&ei=1&en=caf5841999b0d8ca

[ix] *Safeguards Built into Hand Count, Official Says*, by Jim Haley, the Herald, Everett WA, December 14, 2004, http://www.heraldnet.com/stories/04/12/14/100loc_recount001.cfm.

[x] Final Report, Cuyahoga Election Review Panel, Cuyahoga County, OH, July 20, 2006, http://bocc.cuyahogacounty.us/GSC/pdf/elections/CERP_Final_Report_20060720.pdf
[xi] Ibid, page 102.
[xii] Ibid, page 139.
[xiii] Ibid, page 46.
[xiv] Ibid, page 46.
[xv] Ibid, page 50 – 51.
[xvi] Ibid, page 217.
[xvii] Testimony by Mr. Michael I. Shamos before the Committee on House Administration, September 28, 2006.
[xviii] http://www.chicagotribune.com/news/nationworld/chi-0602110098feb11,1,6644357.story or http://www.votetrustusa.org/index.php?option=com_content&task=view&id=913&Itemid=298
[xix] The Primary Election of March 21, 2006 Analysis and Recommendations, April 27, 2006, http://www.ballot-integrity.net/docs/Cook_County_Board_v6_4-26-2006.pdf.
[xx] This quote is footnoted in the original document as follows: Chairman Jesse R. Smart, EBOE, September 19, 2005 – Meeting transcript, page 18.
[xxi] *A Verifiable, Accessible Vote*, by Barbara Silverstone, New York Times, June 14, 2004, http://query.nytimes.com/gst/fullpage.html?res=9A0DE0DE1230F937A25755C0A9629C8B63&n=Top%252fReference%252fTimes%20Topics%252fSubjects%252fE%252fElections
[xxii] August 1, 2006, http://www.votetrustusa.org/index.php?option=com_content&task=view&id=1595&Itemid=804. Also see *My Rationale for Filing an ADA Complaint against the State of Florida*, by A. J. Davies, April 4, 2006, http://www.votetrustusa.org/index.php?option=com_content&task=view&id=1159&Itemid=26
[xxiii] American Council of the Blind of New York, Inc.; Center for Independence of the Disabled in New York (CIDNY); Disabilities Network of NYC; New York State Young Democrats Disability Issues Caucus; Queens Independent Living Center; Westchester Council of the Blind; Westchester Disabled on the Move, Inc. For the full list of endorsements, see http://www.nypirg.org/goodgov/hava/machines/endorsers.html
[xxiv] For the full statement, see http://www.nypirg.org/goodgov/hava/machines/default.html
[xxv] From the oral testimony of Jim Dickson before the Committee on House Administration's hearing entitled, "Electronic Voting Machines: Verification, Security, and Paper Trails," September 28, 2006,
[xxvi] Letter from Kelly Pierce to Interested Persons, dated October 4, 2006. In that letter Pierce references my testimony in which I quote blind computer scientist Noel Runyan as follows: *The experiences of this voter, which were quoted in the report, were shared recently in testimony before a congressional committee.*
[xxvii] "In 2005 Smartmatic acquired Sequoia Voting Systems, a well-known leader among suppliers of electronic voting systems in the U.S. market". Quote taken from *About*

Smartmatic, http://www.smartmatic.com/news_070_2005-10.htm. See also *California: Sequoia Quietly Leading State E-voting*, by Ian Hoffman, originally published in Inside Bay Area, available at http://www.votetrustusa.org/index.php?option=com_content&task=view&id=1411&Itemid=51

[xxviii] Personal correspondence with Noel Runyan, October 3, 2006.

[xxix] Personal correspondence with Noel Runyan, October 4, 2006.

[xxx] Ibid.

[xxxi] *Network administrators can save time and money by letting servers carry the load*, by J. B. Miles, Government Computer News, October 2, 2000, http://www.gcn.com/print/vol19_no29/3040-1.html.

[xxxii] http://www.eac.gov/election_resources/vss.html

[xxxiii] "The MTBF demonstrated during certification testing shall be at least 163 hours", http://vote.nist.gov/VVSG2005Pt1.htm.

[xxxiv] http://www.nytimes.com/2005/01/18/opinion/18tues1.html?ex=1107100499&ei=1&en=caf5841999b0d8ca

[xxxv] For more discussion of equal protection and related issue, see *DRE Reliability: Failure by Design?*, by Howard Stanislevic, March 13, 2006, http://www.votetrustusa.org/pdfs/DRE_Reliability.pdf.

[xxxvi] http://truevotemd.org/Resources/Lessons_Learned.pdf

[xxxvii] The ESD discussion is based on private communication from Stanley A. Klein, October 6, 2006.

[xxxviii] *Fundamentals of Electrostatic Discharge*, ESD Association, Rome, NY, 2001, Table 2, page 5.

[xxxix] *Uncertainty Clouds Future of e-voting Tests*, by Ian Hoffman, Oakland Tribune, December 1, 2005, available at http://www.votersunite.org/article.asp?id=6414.

Forsyth County Elections and Voter Registration

110 E. Main St.
Cumming, Georgia 30040
Tel – 770-781-2118

memo



Date: October 26, 2006

To: Committee on House Administration

From: Gary J. Smith
Director of Elections

Reference: 2006 Hearing on Electronic Voting Machines: Verification, Security, and Paper Trails

I have enclosed the following:

- **My transcript with no changes**
- **Answers to Representative Holt's questions**



Response from Gary J. Smith to Representative Holt's questions – 10/26/06

Committee on House Administration Hearing on electronic Voting Machines:
Verification, Security, and paper Trails
September 28, 2006

Response from Gary Smith to Representative Holt's Additional Questions – 10/25/06

Description of security procedures for Forsyth County Elections. Receipt, Maintenance, and Storage.

(a) Acceptance tests. Upon the receipt of each new direct recording electronic voting unit (DRE), I am responsible to ensure that an acceptance test is performed on the device in accordance with standards issued by the Secretary of State. No DRE unit shall be accepted by our county or placed into service until such time as the unit satisfactorily passes the prescribed acceptance tests.

(b) Storage of DRE units.

1. We maintain our DRE units in accordance with the requirements of this rule, the directives of the Secretary of State, and the specifications and requirements of the manufacturer (Diebold).

2. The DRE units are stored in a climate controlled space in which the temperature and humidity levels are maintained at acceptable levels year-round which shall not be lower than 5 degrees Celsius (41 degrees Fahrenheit) nor higher than 40 degrees Celsius (104 degrees Fahrenheit) and not lower than 35 percent relative humidity and not higher than 85 percent relative humidity such that no condensation forms on such units. The units are not stored in an area in which liquids or fluids stand, pool, or accumulate at any time or in areas that are subject to such standing, pooling, or accumulating liquids or fluids. The space in which the units are stored is secured by multiple security devices and is accessible only to persons authorized by myself to have access to such units or such space. The DRE units are kept on a rack system that has been constructed for the storage of the units. The batteries in each unit are charged at least quarterly in accordance with the manufacturer's specifications.

3. The storage areas for DRE units is equipped with the following forms of electronic surveillance and protection: keypads and electronic locks, motion detectors, video surveillance, and a security system that is connected to an outside monitoring source, in our case the police department and fire department.

4. We maintain numbered seals on all DRE units in storage and all seal numbers shall be recorded and on file in our office.

5. Upon delivery to a polling place in preparation for a primary, election, or runoff, the DRE units are secured and protected from unauthorized access by storing the DRE units in a locked and secure room at the polling place, having the person taking possession of the units personally supervise the units at all times prior to the opening of the polls.

6. Software security. The software contained in each DRE unit, regardless of whether the unit is owned by the county or the state, and the software used to program the unit and to tabulate and consolidate election results has not been modified, upgraded, or changed in any way without the specific approval of the Secretary of State. No other software is loaded onto or maintained or used on computers on which the GEMS

software is located except as specifically authorized by the Secretary of State. Dynamic encryption keys help to secure our election results and we have the ability to change our passwords at each election. Election results are digitally signed to prevent any attempt to tamper with the contents of the memory cards.

(d) Access to GEMS servers.

1. The room in which the GEMS server is located is locked at all times when the server is not directly under my supervision or my designee. Lock and key access to the room where the GEMS server is located is be limited to myself; my election supervisor, and emergency personnel. Building maintenance personnel have access to the room in which the GEMS server is located only to the extent necessary to carry out their maintenance duties and under our supervision. We maintain on file at all times in our office a complete and up-to-date list of all maintenance personnel with access to the room in which the GEMS server is located. Emergency personnel shall have access to the room in which the GEMS server is located only as necessary in the event of an emergency and only for the duration of such emergency condition and in this event, the computer controlled access monitors all ingress and egress as well as the video surveillance cameras.

2. The GEMS server remains locked at all times when not in use. The key or keys to the GEMS server shall remain in the possession of myself and my designee at all times.

(f) Security of DRE units and accessories. All DRE units, optical scanner devices, voter access cards, supervisor cards, memory cards, DRE unit keys, voting system software, and encoders are stored under lock and key at all times when not in use. Lock and key access to such items are limited to myself; my election supervisor; the personnel of my office; building maintenance personnel (under supervision); and emergency personnel. Building maintenance personnel have access to the area where such items are stored only to the extent necessary to carry out their maintenance duties and under supervision of the election staff. I maintain on file at all times in my office a complete and up-to-date list of all maintenance personnel with access to the area in which such items are stored. Emergency personnel have access to the area where such items are stored only as necessary in the event of an emergency and only for the duration of such emergency condition and under video surveillance and computer coded access. Whenever maintenance or emergency personnel are required to enter the storage area, it is required that I be notified in advance and maintain a log of those persons who entered the storage area.

(g) Voting system handling requirements.

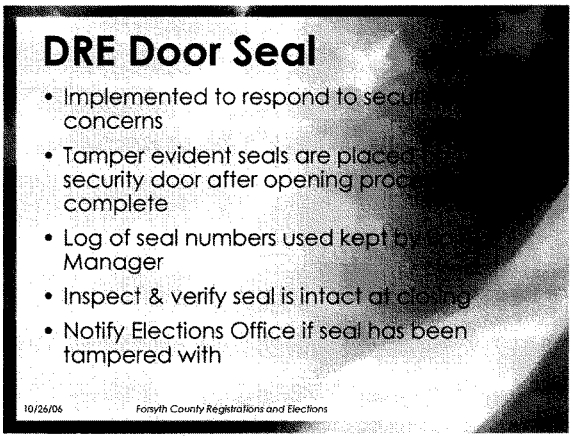
1. All personnel, with the exception of the permanent employees of the Office of the Secretary of State and permanent employees of our county election staff, who prepare voting equipment for use in a primary, election, or runoff complete an oath of custodian before each election. One copy of the oath is placed on file in the office of the election superintendent and an additional copy is filed with the records for the election filed with the clerk of superior court. The oath of custodian is in the following form:

STATE OF GEORGIA
COUNTY OF _FORSYTH
OATH OF CUSTODIANS AND DEPUTY CUSTODIANS
OF DRE UNITS

Response from Gary J. Smith to Representative Holt's questions – 10/26/06

I, _____, do swear (or affirm) that I will as a (deputy) custodian of the voting systems for the County Forsyth, faithfully perform all of my duties in accordance with state law; that I will prepare in accordance with all applicable rules and regulations governing the use of the voting system all DRE units to be used in primaries, elections, and runoffs in this county; that I will use my best endeavors to prevent any fraud, deceit, or abuse in carrying out my duties while preparing the DRE units for use in primaries, elections, and runoffs; and that I am not disqualified by law to hold the position of (deputy) custodian.

Included for reference and visual description are some of the security seals and reports that help to maintain security and chain of custody.



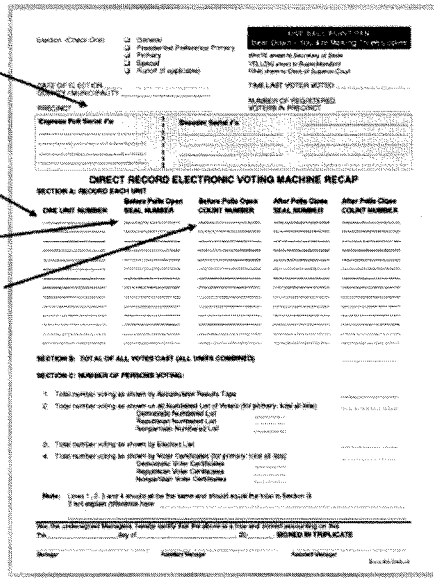


Response from Gary J. Smith to Representative Holt's questions – 10/26/06

CHAIN OF CUSTODY FORMS

DRE Recap Sheet

Opening the Polls

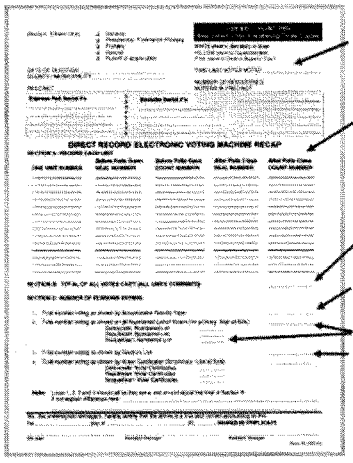


10/23/06

DRE Recap Sheet

Closing the Polls

Declare, "The Polls are Closed" at 7:00 PM. Any voter(s) in line at 7:00 PM must be allowed to vote. Position a Poll Officer at the end of the line to ensure that anyone arriving after 7:00 PM is NOT allowed to vote.



10/23/06 *Forsyth County Registrations and Elections* 15

Response from Gary J. Smith to Representative Holt's questions – 10/26/06

Part of poll worker training to assure voter access cards are not lost -



EXIT DOOR STATION

- Collect Voter Access Cards.
- Give Voter "I Have Voted" Stickers.
- Return used Voter Access Cards to ExpressPoll Station.
- NO Voter should exit without first returning Voter Access Card.

With respect to the comment about counterfeit voter access cards gaining access to the voting process – all Georgia Voter Access Cards in our county are maintained in secured storage and are of a type that is different than those used for training or any of our outreach programs. Although the prior Georgia Voter Access Card may have looked like something used in a Laundromat, the Georgia Smartcard currently used is coded for a specific card style for a specific precinct in our county for a specific election. Attempts to duplicate a commercially available smart card with the information needed to be used in an election have not been successful to our knowledge.

All election systems equipment is part of our inventory for each of our precincts and is a routine part of the equipment delivery and chain of custody. This includes, but is not limited to: dre machine numbers, TS Access Cards, Encoders etc. These are kept on file by precinct, poll manager and issuance date.

Question from Representative Holt – Does confidence in the security and accuracy of your voting systems – confidence among all races equally – matter? Representative Holt quoted the both the 2004 Peach Poll http://www.cviog.uga.edu/peachpoll/2004-01-23.pdf and the 2005 Peach Poll http://www.cviog.uga.edu/peachpoll/2005-03-10.pdf with respect to the confidence of voters.

Confidence in the security, integrity, and accuracy of the Georgia and Forsyth County voting system is of the utmost concern and importance for all voters, regardless of race. Your comment with respect to black voters should show: the recent Peach Poll indicates that statewide black voters had increased by four percentage points as very confident and decreased by two percentage points as not at all confident. In addition, 89% of all of the voters surveyed indicated that they were confident that their vote was counted accurately. As part of the continued advancement in elections in Georgia, we now offer "no excuse" absentee voting by paper ballot for all voters. In addition, we have "early voting" remote sites set up in Forsyth County to help with those who wish to Vote In Person, but are unable to on Election Day. The combination of "no excuse" and "early voting" have proven to be very popular with our county's voters and seemingly with the other counties in Georgia.

Response from Gary J. Smith to Representative Holt's questions – 10/26/06

"And in Georgia, the replacement of the state's hodgepodge of voting equipment with a uniform touchscreen voting system has had an even more dramatic impact, with the statewide rate of uncounted votes declining from 3.5% to .39%.[1] Some of the biggest improvement in 2004 election was in heavily African-American precincts that had formerly used punch cards.[2] Yet despite these improvements, the debate over electronic voting shows little sign of abating". - Doug Gross, *Georgia Election Data Shows Black Precincts Saw Biggest Voting Improvements*, Ledger-Enquirer, Dec. 2, 2004, *at* http://www.ledger-enquirer.com/mld/ledgerenquirer/news/local/10321965.htm; *Id.*; *see also* Charles Stewart III, *The Reliability of Electronic Voting Machines in Georgia*, VTP Working Paper (Oct. 2004), *available at* http://www.vote.caltech.edu/Reports/georgiastewart.pdf.

Question from Representative Holt – If someone walked off with a memory card or a voting machine in your jurisdiction, would you know?

With the security procedures that we have in place, it would not be possible for someone to walk off with a memory card or voting machine in Forsyth County.

I believe some of the following comments should be considered in any review of a contemporaneous paper audit trail.

"Likewise, legislative bodies should avoid mandating any particular technological fix, such as the contemporaneous paper record or "voter verified paper audit trail."[3] A likely effect of that sort of mandate is to disadvantage minority, disabled, and non-English speaking voters. It can also be expected to stifle innovation by locking in a particular type of security enhancement, while discouraging other possibilities that may be more effective and easier to implement." - For one discussion of the "voter-verified paper audit trail," see Kevin Shelley, Cal. Sec'y of State, *Ad Hoc Touch Screen Task Force Report* 21 (2003), *available at* http://www.ss.ca.gov/elections/task_force_report.doc.

"I conclude that, while there are legitimate reasons to be concerned about the implementation of DRE voting, paper should not be considered the gold standard. In particular, it is questionable whether adding printers to DRE machines is either a workable or effective solution to the vulnerabilities that exist." – Daniel Tokaji – page 66 Fordham Law Review – The Paperless Chase: Electronic Voting and Democratic Values

A recent paper by Ted Selker and Jon Goler of Massachusetts Institute of Technology assesses the practical problems with the contemporaneous paper record.[4] They find that:

=xt[The contemporaneous paper record] 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 operation 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.[5]=FT

Implementation of the contemporaneous paper record is thus considerably more difficult than some advocates' public statements might suggest."

In conclusion, with the experience that I obtained in managing the recent manual audit of the VVPAT in Cuyahoga County – I agree with the comment made by Mr. Tokaji –

"The experience of jurisdictions that have attempted to implement DREs capable of generating a contemporaneous paper record illustrates the practical difficulties inherent in making such a system work in a real-world election. Introducing an additional piece of equipment can complicate the voting process, resulting in confusion on the part of both voters and poll workers. The introduction of the contemporaneous paper record has proven to be no exception. And as described below, the device has proved problematic at best in jurisdictions that have attempted to use a contemporaneous paper record system on a limited basis." - Daniel Tokaji – page 77 Fordham Law Review – The Paperless Chase: Electronic Voting and Democratic Values

"Likewise, legislative bodies should avoid mandating any particular technological fix, such as the contemporaneous paper record or "voter verified paper audit trail."[6] A likely effect of that sort of mandate is to disadvantage minority, disabled, and non-English speaking voters. It can also be expected to stifle innovation by locking in a particular type of security enhancement, while discouraging other possibilities that may be more effective and easier to implement. "- For one discussion of the "voter-verified paper audit trail," see Kevin Shelley, Cal. Sec'y of State, *Ad Hoc Touch Screen Task Force Report* 21 (2003), *available at* http://www.ss.ca.gov/elections/task_force_report.doc.

Responses by Michael I. Shamos to
Representative Holt's Additional Questions for Witnesses
Committee on House Administration Hearing on
Electronic Voting Machines: Verification, Security, and Paper Trails
September 28, 2006

Answers to Questions for Michael Shamos

1. I expect you are familiar with the Brennan Center of Justice, working in conjunction with the National Institute for Standards and Technology, Ron Rivest of M.I.T, former White House Cyber Security Advisor for George W. Bush Howard Schmidt, and other security experts. The task force that produced that report conducted an exhaustive and comprehensive analysis of all of the major types of voting systems used in the United States – DREs with VVPAT, DREs without, and optical scan systems. The report concluded that all of the systems were vulnerable to attack and malfunctions, and recommended that voter verified paper records, accompanied by routine random audits be used, and that the use of wireless devices be banned. As my legislation would implement all of those recommendations, I was very pleased not just about the report but also about the endorsement it received from Jeannette M. Wing, President's Professor of Computer Science, Computer Science Department Head, Carnegie Mellon University – "I give my full support for this study. It is important for the nation to preserve our founding principle of democracy, which rests largely on the integrity of how we elect our leaders – our democratic process of voting." Is your Institute for Software Research in the Computer Science Department at CMU?

Answer: I declare at the outset my dismay at the personal enmity displayed by Rep. Holt in the formulation of this entire set of questions. They do not further legitimate congressional inquiry and are not calculated to repair the serious problems that have been identified in the text of H.R. 550. Though I may disagree with the premise of Rep. Holt's bill, and find fault with it, I have never challenged his personal motives or qualifications. I apologize to the Committee to the extent that the tone of my answers has matched the malevolent spirit in which his questions were posed.

I am familiar with the Brennan Center Report. I have read it. I am in general agreement with all of its recommendations, except for that of a paper trail, but I am in extreme disagreement with the logic and fictional scenarios used to arrive at those recommendations. That it has an otherwise impressive list of names associated with it is of no consequence if the report itself is flawed. You know from my testimony that I favor voter verification and random routine audits, and I am one of the loudest voices calling for a ban on wireless components.

Prof. Wing is head of the Computer Science Department at Carnegie Mellon University, which is a division of the School of Computer Science. I have known her for over 20 years. The Institute for Software Research is a co-equal division of the School of Computer Science, but is not part of the Computer Science Department. It does not report to Prof. Wing, and Prof. Wing is not among its faculty. It would not matter if the

situation were otherwise. The value of a report does not derive from its list of endorsers, but from whatever value might be gleaned from its content. I think you will find if you ask Prof. Wing how many voting systems she has examined, she would say zero. I have examined 119 of them, so if appeal to authority were a valid method of argument (which it is not), my opinion on the Brennan Center Report would perhaps be of greater value than hers. CMU's experts on electronic voting, namely me, Lorrie Cranor, David Farber and Alessandro Acquisti, are associated with the Institute for Software Research, not the Computer Science Department. I note with amusement that of the eight "endorsements" publicized by the Brennan Center on its website at http://www.brennancenter.org/programs/downloads/MOD%20Endorsements.pdf, five we furnished by authors of the report, hardly an independent view. Prof Wing was one of three non-author endorsers.

The Brennan Center Report is not a paragon of scientific objectivity. The participants were deliberately selected based on their favorable inclination toward paper trails. I am informed that NIST withdrew its participation when it learned of this, and requested that the Brennan Center remove NIST's name from the report. So the premise of your question, that the Brennan Center worked in conjunction with NIST, is incorrect. Possibly if the reports' external endorsers knew this to be the case they might not have been so free with their praise.

It is no particular surprise that your legislation would implement the recommendations of the Brennan Center Report since the main points H.R. 550 were suggested by some of the very same people who served on the Brennan Center Task Force. The implication that somehow the Brennan Center is therefore an independent supporter of H.R. 550 is incorrect.

2. You identified that "[t]he effect of H.R. 550 would be to ban electronic voting entirely in Federal elections. The reason is that the bill sets forth conditions that are not met by any DRE system currently on the market in the United States. If it were to pass in its present form, there could be no more electronic voting in this country." Section 2 of my legislation provides that every "voting system shall produce or require the use of an individual voter-verified paper record of the voter's vote that shall be made available for inspection and verification by the voter before the voter's vote is cast. For purposes of this clause, examples of such a record include a paper ballot prepared by the voter for the purpose of being read by an optical scanner (whether form a domestic or overseas location), a paper ballot created though the use of a ballot marking device, or a paper print-out of the paper ballots produced by a touch screen or other electronic voting machine, so long as in each case the record permits the voter to verify the record in accordance with this subparagraph." Thus, touch screen machines, optical scan machines and ballot marking devices are all explicitly allowed by my legislation. Can you explain specifically which electronic systems you believe this legislation would outlaw.?

Answer: I believe that H.R. 550 is not quoted correctly in your question. The phrase "paper print-out of the paper ballots produced by a touch screen or other electronic voting

machine" should instead read "paper print-out of the voter's vote produced by a touch screen or other electronic voting machine."

H.R. 550 would outlaw all DRE machines currently on the market in the United States. It would allow optical scan and ballot marking devices which mark optical scan ballots. It is not sufficient to say that "touch screen machines ... are .. explicitly allowed by my legislation." They may be expressly "allowed" but they are implicitly disallowed by the conditions the legislation places on them. For example, I might propose a bill that allows automobiles but requires them to get 150 miles per gallon of gasoline. Since no car achieves this, it implicitly outlaws cars while purporting to permit them. Likewise, your simultaneous requirement for a paper trail and voter secrecy is not currently satisfied by any paper trail machine. All sequential paper trail machines are automatically disqualified. Even Barbara Simons, a staunch paper trail advocate, so testified at the hearing on Sept. 28. The cut sheet machines (such as Avante), print indicia on the ballot, such as codes and identification numbers, that can be used by a voter to identify his ballot.

3. You stated in your testimony that "the bill as written mandates a system that would violate constitutional and statutory provisions in more than half of the states. The secret ballot is regarded as an essential component of American democracy. Each one of the DRE paper trail systems that are currently on the market either enables voters to sell their votes, or allows the government and the public to discover precisely how each voter in a jurisdiction has voted. I cannot believe that the numerous sponsors of this legislation contemplated such an outcome." The sponsors of HAVA already required a "permanent paper record with a manual audit capacity," and the DREs you have certified for use in Pennsylvania presumably meet that requirement or I assume you would not have certified them. Can you explain how it is that the internal paper record produced by those DREs (which is not verifiable by voters) preserves the privacy of voters, while an external version of the same thing (which is verifiable by voters) does not? If either voters are randomly shuffled (directed to different voting booths) or the paper records are shuffled by each machine, do you think the secrecy of any voters ballot is compromised?

Answer: It should be noted that I do not certify voting systems. I examine them and write reports recommending a grant or denial of certification. My reports are reviewed by the Pennsylvania Commissioner of Elections, the state's HAVA Coordinator, the counsel for the Department of State and the Secretary of the Commonwealth. It is the Secretary who makes the ultimate decision on certification. I do not deny that I have a significant role in the process, but my recommendations are subject to extensive review.

All machines certified in Pennsylvania have the capability of producing a "permanent physical record of each vote cast, as required by 25 P.S. §3031.1. This requirement was enacted in 1980, predating HAVA by 22 years. They also satisfy the HAVA requirement of a "permanent paper record with a manual audit capacity for such system." 42 U.S.C. §15481(a)(2)(B)(i). This is done in different ways by different vendors, but in general it consists of maintaining ballot images (cast vote records) in randomized order so they cannot be associated with any particular voter. The file of ballot images (randomized) can be printed out after the close of polls either at the original voting machine or at

county central after results have been uploaded, or both. Sequential paper trail machines cannot shuffle any ballots and are completely non-random. Thus they are not an "external version of the same thing," as your question suggests.

Shuffling the paper records produced by the cut-sheet machines is not sufficient since each ballot has a unique identification code. Directing voters to different voting booths does not work for several reasons: (1) In Massachusetts, for example, DREs are used only for the disabled and no polling location has more than one machine. Therefore, the ballot of every disabled person is exposed in a recount; (2) HAVA itself provides that its accessibility requirements can be satisfied by having a single accessible machine in each polling place; (3) Even if there is more than one machine, there is no law that prevents any citizen from remaining in the polling place all day long and recording the machine on which each voter votes. But it is not even necessary to go to such lengths. Voter privacy forbids anyone from knowing how even one voter voted. So if someone watched which machine the first voter of the day used, that vote would be exposed. Likewise, if the machine on which the last voter voted is known, that voter's choices would also be exposed; (4) In some jurisdiction, such as Pennsylvania, the law requires the judge of elections to assign a sequential number to voter and to record that number on the poll list. This provides a one-to-one mapping between voters and the sequential paper trail.

The fact that one or two small vendors produce cut-sheet VVPATs is of only minor consequence. The VVPAT systems of all the major manufacturers, Diebold, ES&S, Sequoia and Hart InterCivic, are all sequential. Replacing those systems, as H.R. 550 would require, would cost additional billions of dollars.

4. I understand you were instrumental in Pennsylvania's certification of the Diebold TSx.

a. Have you verified that the Diebold TSx does not have the same class of vulnerabilities as those described in the Diebold TS by Felten and his students?

b. If so, please explain what Diebold had done to address these vulnerabilities and why you believe these steps to be sufficient.

c. If not, did you recommend that Pennsylvania certify this machine? Why did you make the recommendation that you did?

Answer: I was the examiner for the Diebold TSx and I recommended that it be denied certification following an examination in July 2005. I recommended its certification after a re-examination in November 2005. The certification was granted by the Secretary of the Commonwealth, pursuant to statute, not by me.

a. The Diebold TSx exhibits one of the vulnerabilities identified by Harri Hursti and subsequently studied by Prof. Felten. A knowledgeable intruder who gains access to the machine in secret is able to replace its software. The viral spread identified by Felten on the TS is not possible on the TSx because replacement of the software requires user acknowledgement on the TSx, so the software cannot spread without human cooperation.

b. I am not a spokesperson for Diebold. However, I am informed that Diebold has submitted a new version of TSx for ITA examination that would eliminate the vulnerability. I am further informed that testing on this version is not yet complete. Since I do not know what solution has been implemented by Diebold, I can't say whether or not it is sufficient.

c. When I recommended that the machine be certified in January 2006, these vulnerabilities had not yet been discovered. The system had been federally qualified and passed all tests for conformance with state law. There was no rational basis on which to deny certification. Had the Secretary denied certification when the system conformed to the requirements of HAVA and Pennsylvania law, a vendor lawsuit to reverse such a clearly erroneous determination would have been successful.

5. You acknowledge that security vulnerabilities have been demonstrated by Hursti, Felten and others. You go on to say, "Some of these vulnerabilities are severe and require immediate repair. But the point is that they are easily remedied."

d. If so, why were they security vulnerabilities not remedied initially?

e. How do you know that the security vulnerabilities that have been uncovered by computer security experts have not already been exploited to rig elections? Precisely how do you prove that election rigging has not already occurred using paperless DREs.

f. You assert that the vulnerabilities are easily remedied. Please explain in detail just how to remedy *easily* the vulnerabilities uncovered by Hursti, Felten, et al.

g. Even if the security vulnerabilities were easily remedied, how will the remedies be applied to the voting systems currently in use? Please respond in particular to the fact that one of the vulnerabilities uncovered by Felten requires changes to the hardware in order to be remedied.

Given that independent computer security experts such as Rubin, Felten, and Hursti have been able to examine only Diebold machines, how do you know that similar security vulnerabilities don't exist on DREs produced by other vendors?

Answer:
d. The security vulnerability Hursti II/Felten was remedied in Pennsylvania immediately after it was discovered. Pennsylvania is the only state in which I had sufficient influence to urge such a step successfully. Hursti I, relating to use of AccuBasic on optical scan memory cards, has not been remedied and the system that exhibits that vulnerability (Diebold AccuVote OS) was denied certification in Pennsylvania.

e. The answer is simple. Since there are no paperless DREs in Pennsylvania, no election has ever been held using them, so no election could have been rigged on a paperless DRE. All DREs have paper audit trails, but they are not necessarily shown to the voter. I

presume you mean a DRE with a VVPAT. DREs with VVPATs do not necessarily expose election rigging, either, unless every voter check the paper trail and the paper is used to recount the election. The mere existence of a VVPAT may deter, but does not prevent, rigging.

I don't know whether the vulnerabilities have ever been exploited to rig a DRE election, but there is no evidence that they have been. I can't prove it, but neither is there any statute or regulation requiring such proof. To believe that rigging has occurred, one must give credence to a very unlikely, but not impossible, series of events: (1) the intruder must craft a program that only behaves badly during an election, and at no other time; (2) the intruder must leave no evidence of tampering, physical or otherwise; (3) the intruder must choose carefully how many or what percentage of votes to swap so as not to arouse undue suspicion; (4) the intruder must arrange to affect enough machines to alter the outcome of an election; (5) the intruder must cause his program to erase any trace of itself and replace itself with the authorized software without leaving any evidence; and (6) every intruder who has ever attempted such an intrusion must have succeeded perfectly, or we would have evidence of his attempt. It's not impossible, but there is no reason whatsoever to believe it has happened. One might ask for proof that Martians are not living among us. There's no proof they aren't, but there's no credible evidence that they are, either. Meanwhile, the whole time that people have been arguing over the security of DREs, real elections have regularly been stolen through simple manipulation of paper ballots. This has always been true and it remains true today. For an illuminating treatment, see "Deliver the Vote: A History of Election Fraud, an American Political Tradition, 1742-2004," by Tracy Campbell (2005).

f. Prof. Felten is proud to demonstrate that he can rig a voting machine in one minute. In Pennsylvania we used the very same method to unrig the voting machines (assuming they had been rigged) in a minute. As I explained during my testimony, 16 copies of the certified software were obtained on memory cards from the ITA, one for each Diebold county in Pennsylvania. The copies were individually distributed to those counties. They were instructed at the time when the machines were to be prepared publicly for the election to insert the authorized memory card and answer "yes" to the questions asking whether to replace the machine's firmware and software. This was done for each machine in each of the 16 counties. At this point the machines had the authorized, certified software. If anyone had previously tampered with them, and there was no evidence that anyone had, the effect of the tampering would have been nullified.

Hursti I, involving report generation software on opscan memory cards, is easily remedied be either disabling the AccuBasic mechanism or digitally signing the AccuBasic files. Since this has not yet been done by the vendor, the machines affected by the vulnerability are not certified in Pennsylvania.

g. The answer to (g) is the same as my answer to (f). In some cases, field re-installation of the certified software is required for each machine. The vulnerability identified by Prof. Felten that he says requires a hardware change is the fact that someone who gains access to the machine can replace various physical components within, including ROM

chips, and in effect transform the machine into a totally different machine. That is of course correct, and it applies to every computer system on Earth. The argument applies equally well to paper trails and bank vaults. Someone who has access to the paper trail can alter it; someone who has access to the bank vault can remove the money. Therefore, it is important to keep people away from voting machines and bank vaults.

One might equally imagine entire impostor machines being substituted for the real ones, and equally fanciful hypotheses. The fact that someone is able to dream up a hypothetical attack does not mean that we need to discard DREs, and it certainly does not mean that we need to require paper trails, which now after field testing have shown themselves to be unwieldy and unreliable. In many cases the remediation of security problems consists not in software changes but in application of administrative and physical procedures.

Re: similar vulnerabilities on other machines. The identified vulnerabilities depend on architectural aspects of the Diebold systems that are not shared by any other systems.



Michael I. Shamos

The CHAIRMAN. Welcome, Representative Holt. We are pleased to have you here. This is one of the few times in the Congress when you will find two physicists sitting at the front desk listening to testimony.

At this time, I would like to recognize the Ranking Member, Ms. Millender-McDonald, for any opening remarks she may have.

Ms. MILLENDER-MCDONALD. Thank you, Mr. Chairman, and good morning to you and all the witnesses and guests here this morning. I would like to thank you, Mr. Chairman, for calling this very important hearing on electronic voting machines. I am sure that you have heard from your constituents and constituents around the country, as I have heard, that folks are wary about these voting machine apparatuses and they are not sure whether or not they are working.

Let me also thank you, Mr. Chairman, for welcoming Congressman Russ Holt to sit on the panel this morning. It was just 6 years ago that the 2000 Presidential election brought to light many problems with the elections process in our country. We encountered a wide range of frustrations with the election administration. Some of the most infamous problems involved punch cards with all of the hanging chads that the Chairman has just shown you. Others involved voters who were turned away from the polls without the opportunity to cast a vote.

In response, this committee worked diligently and passed the Help America Vote Act, which is HAVA, to rid the country of outdated voting equipment and to ensure no eligible voter is turned away from the polls without casting a vote. Despite the passage of HAVA, however, many problems still remain, as we witnessed during the 2004 election and in several primaries this year.

Today I hope to hear about methods of addressing these issues, even if we may not be able to implement suggested recommendations before the November election. I also hope that this oversight hearing will serve as a forum for the American people to gain confidence in direct recording electronic voting system machines.

After the 2000 election, DRE, as we call them, machines were viewed as the answer to hanging chads and century-old lever machines. DRE machines also allowed individuals with disabilities to vote in private and without assistance for the first time. They have also been supported by a number of civil rights organizations, given the ease with which they are able to be programmed to display ballots in foreign languages.

However, as we are aware, many concerns have been raised about the integrity and the reliability of these DRE machines. In fact, at times it may be seen that these machines have raised many more questions than answers. For example, some have called for a voter-verified paper audit trail for DRE machines. Some States already require this function for DRE machines.

But even this similarly simple method raises numerous concerns. For example, when mechanisms serve as the official—what mechanism serves as the official record in a recount? That is a question that has been raised often. What happens when the printer jams? Would the votes which were properly recorded by the DRE be thrown out if they are not similarly recorded on the paper? Those are the questions that have been raised often.

I am also interested in hearing from our witnesses, especially the local election officials, regarding their views about the wisdom of imposing a Federal mandate which would specify which type of election equipment should be used. These decisions have mostly been left up to the State and local officials throughout our country's history, and I would like to know what the impact of a Federal mandate and a standard in this area would be, what precedent it would set for future election administration mandates on the States by the Federal Government, and how these mandates would be funded.

In addition to discussing established concerns about DRE machines, I hope the witnesses invited today will address the security of all voting equipment. Only one-third of Americans will cast ballots on DRE machines, and although that number is growing, it still means that two-thirds of our voters will be casting ballots using other methodologies. Are these machines secure, are they reliable, are they subject to a suitable level of scrutiny?

I am concerned that all of the media attention to voting security will inadvertently discourage voters from going to the polls, resulting in voter suppression. As we witnessed a few weeks ago in Maryland, voting machine reliability, stability and accuracy was not the inherent cause of mayhem. The lack of poll-worker training and other human factors of election administration caused problems and confusion at the polls for both voters and poll workers. If we do not adequately address all of these issues, voters may feel as if their votes will not be counted and decide not to participate on election day.

This is one reason why I offered an amendment to double the funding for the college poll-worker training program. This program encourages college-age students to serve as poll workers and to become more involved with the election administration process.

The electoral process is not perfect, Mr. Chairman. Improvements to the electoral process itself still need to be made. Fortunately, the Help America Vote Act of 2002 is a solid foundation upon which we can institute further electoral improvements. HAVA made it easier for voters to cast a ballot and harder for people to knowingly commit crime and fraud, which is why we need to appropriate the remaining $800 million balance which was authorized in title 2 of HAVA to fully fund the States and give HAVA a chance to work.

As I have stated in the past, it is guaranteed that your vote will be lost if you don't cast a ballot. I would encourage every eligible voter to cast a ballot, no matter how harsh the rhetoric about the November elections and no matter how that ballot is cast: by DRE machines, absentee ballots, provisional ballots or whatever. Americans need to get out in November with the confidence that their vote will be counted correctly. Exercising this precious right is more important than the outcome of the elections, Mr. Chairman.

I hope we can convene additional hearings in the future to examine any shortcomings in election administration and any impediments that voters experience in exercising their constitutional rights.

I look forward to working with the Chairman and other members to continue to improve the voting process and I will continue to

seek full funding of the Election Assistance Commission title 2 grants to ensure that the EAC can continue its crucial work to improve the electoral process. Even if one voter is disenfranchised, that is one voter too many. Thank you, Mr. Chairman.

[The information follows:]

CHA Oversight Hearing on
Electronic Voting Machines: Verification, Security, and Paper Trails

September 28, 2006

10:00 AM
1310 Longworth House Office Building

OPENING STATEMENT OF REP. JUANITA MILLENDER-MCDONALD, RANKING MEMBER

Good morning Mr. Chairman, witnesses and guests. I want to thank the Chairman for calling this very important hearing on electronic voting machines. It was just six years ago that the 2000 Presidential election brought to light many problems with the elections process in our country. We encountered a wide range of frustrations with election administration. Some of the most infamous problems involved punch cards with hanging or pregnant chads. Others involved voters who were turned away from the polls without the opportunity to cast a ballot. In response, this Committee worked diligently and passed the Help America Vote Act (HAVA) to rid the country of outdated voting equipment and to ensure that no eligible voter is turned away from the polls without casting a ballot.

Despite the passage of HAVA, many problems still remain, as we witnessed during the 2004 election and in several primaries this year. Today I hope to hear about methods of addressing these issues, even if we may not be able to implement suggested recommendations before the November election. I also hope that this oversight hearing will serve as a forum for the American people to gain confidence in direct recording electronic voting system (DRE) machines.

After the 2000 election, DRE machines were viewed as the answer to hanging chads and century-old lever machines. DRE machines also allowed individuals with disabilities to vote in private and without assistance for the first time. They have also been supported by a number of civil rights organizations given the ease with which they are able to be programmed to display ballots in foreign languages. However, as we are aware, many concerns have been raised about the integrity and reliability of these DRE machines. In fact, at times it may seem that these machines have raised many more questions than answers.

For example, some have called for a Voter Verified Paper Audit Trail for DRE machines. Some states already require this function for DRE machines. But even this seemingly simple method raises numerous concerns. For example, what mechanism serves as the official record in a recount? What happens when the printers jam? Would the votes which were properly recorded by the DRE be thrown out if they are not similarly recorded on the paper?

I am also interested in hearing from our witnesses, especially the local election officials, regarding their views about the wisdom of imposing a federal mandate which would specify what type of election equipment should be used. These decisions have mostly been left up to state and local officials throughout our nation's history and I would like to know what the impact of a federal standard in this area would be, what precedent it would set for future election administration mandates on the states by the federal government, and how these mandates would be funded.

In addition to discussing established concerns about DRE machines, I hope the witnesses invited today will address the security of all voting equipment. Only 1/3 of Americans will cast ballots on DRE machines, and although that number is growing, it still means that 2/3 of our voters will be casting ballots using other methods. Are these machines secure? Are they as reliable? Are they subject to a suitable level of scrutiny?
I am concerned that all of the media attention to voting security will inadvertently discourage voters from going to the polls, resulting in voter suppression. As we witnessed a few weeks ago in Maryland, voting machine reliability, security, and accuracy were not the inherent causes of mayhem. The lack of poll worker training and other human factors of election administration created problems and confusion at the polls for both voters and poll workers. If we do not adequately address all of these issues, voters may feel as if their votes will not count and decide not to participate on Election Day. This is one reason why I offered an amendment to double the funding for the college poll worker training program. This program encourages college-age students to serve as poll workers and to become more involved with the election administration process.

The electoral process is not perfect. Improvements to the electoral process itself still need to be made. Fortunately, the Help America Vote Act of 2002 (HAVA) is a solid foundation upon which we can institute further electoral improvements. HAVA made it easier for voters to cast a ballot and harder for people to knowingly commit fraud, which is why we need to appropriate the remaining $800 million dollar balance, which was authorized in Title II of HAVA, to fully fund the states, and give HAVA a chance to work.

As I have stated in the past, it is guaranteed that your vote will be lost if you don't cast a ballot. I would encourage every eligible voter to cast a ballot, no matter how harsh the rhetoric about the November elections, and no matter how that ballot is cast – by DRE machine, absentee ballot, provisional ballot or otherwise. Americans need to get out and vote in November with the confidence that their votes will be counted correctly. Exercising that right is more important than the outcome of the elections, Mr. Chairman. I hope we can convene additional hearings in the future to examine any short coming in election administration, and any impediments that voters experience in exercising their constitutional rights.

I look forward to working with the Chairman and other Members to continue to improve the voting process and I will continue to seek full funding of the Election Assistance Commission Title II grants to ensure that the EAC can continue its crucial work of

improving the electoral process. Even if one voter is disenfranchised, that is one voter too many.

Thank you again, Mr. Chairman, for convening this hearing. I look forward to hearing the testimony of all the witnesses.

###

The CHAIRMAN. I thank the Ranking Member for her comments, and I especially want to reinforce something you said. Voting in this nation has traditionally been controlled and operated by the local municipalities, cities, townships, counties and by the states. The only reason the federal government entered this is because of the problems with a federal election of a president in 2000, and we continue to have great respect for the localities and the States which have the responsibilities for implementation. We are simply trying to establish standards only for the federal elections.

Ms. Lofgren, do you have an opening statement?

Ms. LOFGREN. Thank you, Mr. Chairman. I am glad that we are having this hearing today and delighted that we are joined by our colleague, Mr. Holt, the author of H.R. 550. I am inclined to think that Mr. Holt's approach is the right one, but I have declined to be a coauthor of this bill until this hearing because I wanted to try and keep an open mind on this subject and listen to the witnesses, without being a coauthor of the bill. But coming from Silicon Valley, you can imagine that I have had considerable input from people who are quite skilled, and I guess the question that needs to be answered is can this election be hacked.

There are many issues, I am sure we will get into them today, but the integrity of the election process is absolutely essential to the sustenance of a vigorous democracy. Elections do count, as we know. And the direction that our country is going in will be decided by elections. If we can't know for a certainty that that process is not corrupted, then it really goes to the core of the spirit of our Nation and our future as a democracy.

So I realize we are not in a markup mode here today, we are here to get information. I am going to listen very carefully to all the witnesses, but I am hopeful that we could take quick action because this—my own State of California has already moved in the direction that Mr. Holt is suggesting with the verifiable paper audit trail. We need to be able to let the voters of America know that their elections are on the up-and-up and their vote really does count and the election has not been hacked.

So with that, Mr. Chairman, I thank you for holding this hearing and I will yield back because I am eager to hear a very large panel of witnesses before we are called to vote. Thank you very much.

The CHAIRMAN. Thank you for your statement.

Mr. Holt's statement will be entered into the record as we mentioned earlier.

In setting up the panel for this hearing I was determined to try to get the broadest representation possible. I would have had to have 27 witnesses to totally accomplish that, but the fact is that we have tried very hard, as indicated by the large number of witnesses we do have.

I am very pleased with the quality of the witnesses who agreed to appear and we now turn to Dr. Felten for his testimony. He is a professor in the Department of Computer Science at Princeton University, which also happens to be Mr. Holt's district. He recently completed a study of an electronic voting system and will give us a report on his findings. I also understand you have a demonstration for us, Dr. Felten. You may begin.

STATEMENT OF EDWARD W. FELTEN, PROFESSOR, DEPARTMENT OF COMPUTER SCIENCE, PRINCETON UNIVERSITY

Mr. FELTEN. Thank you, Mr. Chairman, and members of the committee for the opportunity to testify today——

Ms. LOFGREN. Mr. Chairman, there are lights on that. Is there a way—much better.

Mr. FELTEN. From a security standpoint what distinguishes computerized voting systems from traditional systems is not that computers are easier to compromise but that the consequences of compromise can be so much more severe. Tampering with an old-fashioned ballot box can affect a few hundred votes at most, but injecting a virus into a single computerized voting machine can potentially affect an entire election.

Two weeks ago my colleagues, Ariel Feldman and Alex Halderman, and I released a detailed security analysis of this machine, the Diebold AccuVote-TS which was used in Maryland, Georgia, and elsewhere. My written testimony summarizes the findings of our study.

One main finding is the machines are susceptible to computer viruses that spread from machine to machine and silently transfer votes from one candidate to another. Such a virus requires moderate computer programming skills to construct. Launching it requires access to a single voting machine for as little as 1 minute.

I will now demonstrate this using a virus we constructed in our laboratory. We have set up here a simulated election for President between George Washington and Benedict Arnold. It is election day morning and we just opened the polls. No votes have been cast yet. I will start by casting the first vote. When I checked in at the polling place at the front desk, the poll worker gave me this voter card which I now insert into the machine. I press the start button and I choose to cast my vote for George Washington. The machine asks me to confirm my choice and I confirm my choice and cast my ballot.

The second vote is similar. I insert another voter card, I choose George Washington again, and again I confirm and cast my ballot. The third voter inserts another voter card and votes again for George Washington. The correct vote count in this election obviously is George Washington, three; Benedict Arnold, zero.

Now it is the close of election day. A poll worker inserts a special supervisor card into the machine, enters a PIN code, and tells the machine to end the election and tally the votes. The machine will now print out a paper tape summarizing the ballot count. When I cast my votes earlier my choice of candidate was recorded in the machine's electronic memory. This record of my vote was invisible to me. I had no way of verifying whether it was recorded correctly or whether it was changed after it was recorded.

In this machine the records were modified by our virus. This paper tape printed out by the machine reports the elections result. It shows George Washington with one vote and Benedict Arnold with two. Every record in the machine and outside the machine is consistent with this fraudulent result.

Our technical report referenced in my written testimony goes into considerable detail about this problem and explains why existing election procedures are not sufficient to prevent it. One lesson

is that security depends on getting the technical details right. Too often the designers of this machine fail to get the details right. A good example is the access door here on the side of the machine. It protects the removable memory card that stores the votes, so the door should be locked securely and access to the keys should be strictly limited; but in fact tens of thousands of AccuVote machines can all be opened with the very same key, and this very same key is used widely in office furniture, jukeboxes and even hotel minibars. It is easily purchased on the Internet. This one I bought online from a jukebox supply shop and it does open the machine.

The implications of our study go beyond just this machine and reveal broader systemic problems. More worrisome than any specific vulnerability is that this system, despite its many problems, was certified, purchased and deployed by many States and counties and has been used in important elections.

We can do more to improve the security of our e-voting. I detail many recommendations in my study and written testimony, but one important safeguard is a voter-verified paper audit trail. A well-designed paper trail can improve security and enhance voter confidence without compromising accessibility. Certainly paper records have their drawbacks, but they have different failure modes than electronic records do and the combination of electronic and paper records can be more robust against fraud than either one would be alone.

Getting the details of voting right is difficult, especially in today's high-tech polling place, but failure is not an option. The stakes are too high and the risk of malfunction or fraud too great to make our current course tenable in the long run.

Election experts, accessibility experts, and computer security experts all have a role to play in improving our voting system. If we work together we can solve this problem and give the American people the voting system they deserve.

Thank you for your time and attention.

The CHAIRMAN. Thank you very much for your testimony.

[The statement of Mr. Felten follows:]

Testimony of Edward W. Felten
Professor of Computer Science and Public Affairs, Princeton University

United States House of Representatives, Committee on House Administration
Hearing on
Electronic Voting Machines: Verification, Security, and Paper Trails
September 28, 2006

Open the lid of an electronic voting machine and look inside; what you will see is a computer, much like an ordinary desktop PC or Mac. Because they are computers, e-voting machines are susceptible to familiar computer problems such as crashes, bugs, mysterious malfunctions, data tampering, and even computer viruses. The question is not whether we can eliminate these problems – we cannot – but how we will cope with them.

Unlike ordinary desktop computers, e-voting systems are entrusted with the most important process of our democracy – collecting and counting votes – and must perform that process accurately, reliably, accessibly, and securely. Trust in election outcomes is necessary for our electoral system to work, but the political system often does not lend itself easily to trusting relationships. Voting technologies must help to build this trust. Today's e-voting infrastructure is not up to the task, but tomorrow's can be.

Two weeks ago Ariel J. Feldman, J. Alex Halderman, and I released a paper analyzing in detail the security of the Diebold AccuVote-TS, one of the most widely used e-voting systems. The main findings of our study were as follows:

1. Malicious software running on a single voting machine can steal votes with little if any risk of detection. The malicious software can modify all of the records, audit logs, and counters kept by the voting machine, so that even

careful forensic examination of these records will find nothing amiss. We have constructed demonstration software that carries out this vote-stealing attack.

2. Anyone who has physical access to a voting machine, or to a memory card that will later be inserted into a machine, can install said malicious software using a simple method that takes as little as one minute. In practice, poll workers and others often have unsupervised access to the machines.
3. AccuVote-TS machines are susceptible to voting-machine viruses — computer viruses that can spread malicious software automatically and invisibly from machine to machine during normal pre- and post-election activity. We have constructed a demonstration virus that spreads in this way, installing our demonstration vote-stealing program on every machine it infects.
4. While some of these problems can be eliminated by improving Diebold's software, others cannot be remedied without replacing the machines' hardware. Changes to election procedures would also be required to ensure security.

Our web site at http://itpolicy.princeton.edu/voting has links to our full technical report and a ten-minute video showing our demonstration vote-stealing virus in operation. The technical report goes into considerable detail and includes a discussion of why existing election procedures are not sufficient to prevent virus attacks. While we are not alleging fraud in any specific past election, our results do raise serious concern about the security of future elections.

One lesson of our study is that security depends on getting the technical details right. A security measure that sounds robust in the abstract may be useless or worse if implemented poorly. Too often, the designers of the AccuVote-TS failed to get the details right.

A good example is the AccuVote-TS access door. The access door on this machine protects the removable memory card that stores the votes, so the door should be locked securely and access to the keys should be strictly limited. In fact, the tens of thousands of AccuVote-TS machines can all be opened with the same key, and this very same key is used widely in office furniture, jukeboxes, and even hotel minibars. I bought several keys on the Internet from an office furniture shop and a jukebox supply shop, and they all open the AccuVote-TS. Details matter. It is not enough to have a key; it matters which key you use.

Some voting machines, including the AccuVote-TS, record votes internally in a computer file, with the votes stored in the order they were cast. This approach endangers the secrecy of the ballot. If election procedures record the order in which voters cast their votes (or allow partisan observers to do so, as is the practice in my polling place), then a sequential record of the votes can be correlated with the order of voters to reconstruct the ballots cast by individual voters. The AccuVote-TS is one voting machine that gets this detail wrong.

The AccuVote-TS suffers from many such problems. It encrypts stored votes, but stores the secret decryption key where it is easily found by hostile software. It keeps two redundant copies of each stored vote, but both copies are subject to easy tampering.

Some of these errors are more technical in nature than the access-door key error and the vote-recording error, but they are just as serious.

The implications of our study go beyond the specific voting machine we studied to reveal broader systemic problems. More worrisome than any specific vulnerability is that, despite its many problems, the system we studied was certified, purchased and deployed by many states and counties, and is slated for use in the upcoming November election. This leads us to conclude that existing certification and procurement procedures are inadequate to prevent the kinds of serious vulnerabilities we discovered. Here again the details matter, and too often current processes get the details wrong.

Though some claim that election procedures will prevent the kinds of problems we identified, the rigid procedures described in vendor manuals are often ignored in practice. Machines are supposed to be sealed with numbered security tape; but missing or broken tape is usually ignored, and election workers often break the tape themselves when trying to revive malfunctioning machines. Machines and removable vote-storage media are theoretically kept under lock and key, but in practice they are often sent home with election workers or left unattended. At my polling place in Princeton, the night before an election, the DRE machines sit unattended in an unlocked elementary school lobby where anyone could tamper with them. Stringent official procedures only matter if they are followed in practice.

There are several things we can do to improve the security of our e-voting infrastructure.

In the short term, some limited steps are still feasible before November. Given the susceptibility of some e-voting systems to electronic tampering, we should take extra care to secure the chain of custody for voting machines and vote-storage media from now until Election Day. This cannot repair machines that have already been tampered with, but it can reduce the likelihood of further tampering. Needless to say, what we need is not more memos laying down theoretical procedures, but detailed execution to narrow the gap between procedural theory and practice.

In the medium term, I offer three recommendations. First, we should fix the certification process to better account for security. Certification seems to focus on machine attributes that are easily tested, but security problems are difficult to detect by testing because no predetermined set of test scenarios can account for the tactics of a clever adversary who systematically exploits gaps in a system.

In practice, the certification process often misses security problems that are simple but very dangerous. For example, the AccuVote-TS system we studied will silently accept and install any software update offered by any memory card that is inserted into the system. The system makes no effort to verify that the offered update is authorized by the vendor, election officials, or anyone else. This is a very serious weakness that opens the door to the injection of malicious software and the silent, automatic spread of viruses. Yet the system was certified despite this obvious vulnerability. The existing certification process seems unable to detect such problems reliably. It must be improved.

Second, a voter-verified paper audit trail (VVPAT) is a necessary safeguard given the state of the art today. With these paper trails, as with other voting

technologies, we must get the details right – poorly designed paper trails can be unreliable or hard to use, or can compromise the secrecy of the ballot – but a well-designed paper trail can improve security and enhance voter confidence, without compromising accessibility.

In comparing VVPATs with paperless DREs, we must compare apples to apples. For example, we must not compare a VVPAT that compromises the secret ballot by recording votes in the order cast (e.g., on a continuous roll of paper) with a paperless DRE that gets this detail right. Instead, we must assume good engineering in both cases, and weigh the significant security benefits of VVPATs against their costs.

Paper records, either VVPATs or traditional paper ballots, have their drawbacks. They are not immune to fraud. What is important is that they have different failure modes than electronic records, so that the combination of electronic and paper recordkeeping, if implemented well, can be more robust against fraud than either would be alone.

One aspect of a well-implemented VVPAT system is that the electronic and paper records must be compared to each other. We do not need to verify every paper record, just enough to detect large-scale fraud. Unless an election is very close – which will probably trigger a full recount anyway – checking a few percent of ballots will suffice. Similarly, it is not necessary for every voter to read and verify the paper record of his vote; as long as even a few voters do so, any tampering widespread enough to be significant will be easily detected.

Third, we must do more to leverage the expertise of independent security experts. Independent analyses, by experts neither paid by nor reporting to voting machine

vendors, have discovered many areas for improvement in today's technologies, yet most vendors systematically try to prevent such analyses. For example, my colleagues and I would be happy to examine other versions of Diebold's AccuVote-TS or AccuVote-TSx software to determine whether they are subject to the vote-stealing virus problems we have identified; but Diebold refuses to let election officials call on us for this purpose. Other vendors follow a similar policy of resisting public study and discussion of the technologies that count our votes.

In the long run, further research is needed to help us understand how to improve the voting system. For example, fully electronic verification technologies may one day be a viable substitute for VVPATs, once researchers have worked out the details necessary to deploy them in the real world accessibly and securely. We also need more systematic studies of what really happens in polling places, especially when problems arise. Finally, there is much to learn from work in other areas of computer security – today, even video game consoles like the Xbox are more tamper-resistant than voting machines.

Those not versed in computer security can miss the significance of e-voting security vulnerabilities. From a security standpoint, what distinguishes computerized voting systems from traditional systems is not that computers are easier to compromise, but that the consequences of compromise can be so much more severe. Breaking into an old-fashioned ballot box can affect a few hundred ballots at most; injecting a virus into a single computerized voting machine can affect an entire election.

Intuitions developed with older technologies can mislead when applied to

computerized systems. For example, non-experts often fail to appreciate how difficult it is to tell what is happening inside a computer system. We cannot "just look" to see what is happening or whether the right software is installed. Often our only recourse is to ask the system itself what it is doing – which is fine if the system is working correctly, but fruitless if the system is compromised. There is no point in asking a virus whether a virus is present.

Similarly, non-experts often assume that pre-election testing is an effective way to trigger and detect malicious software that might have infected a voting machine. Here again, computerized systems are different. A modified lever machine will work the same whether or not it is Election Day; but malicious software on a DRE can check whether the machine is in pre-election testing mode, or can check the date, or can check whether the number and pattern of voters is consistent with election day, and can activate its vote-stealing capability only in a real election. Our demonstration AccuVote-TS virus takes measures to remain inactive and thus evade detection during pre-election logic and accuracy testing. It is very difficult to tell whether such a virus is present. In general, malicious software is much harder to detect than non-experts would expect.

My point is not that these challenges are insurmountable but that one needs specialized knowledge and sophisticated analysis to figure out what is possible. Acknowledging that security experts can learn from election experts, I submit that election experts can also learn from security experts.

Getting the details of voting right is difficult, especially in today's high-tech polling place. But failure is not an option. The stakes are too high, and the risk of

malfunction or fraud too great, to make our current course tenable in the long run. We need to work harder and smarter, exploiting the knowledge of both election experts and technical experts.

Biography of Edward W. Felten

Edward W. Felten is Professor of Computer Science and Public Affairs, and Director of the Center for Information Technology Policy, at Princeton University. His research interests include computer security and privacy, Internet software, and information technology policy. He has published more than eighty papers in the research literature, and two books, and he is widely quoted in the press as an expert on security, privacy, and information technology policy. He has advised the U.S. Departments of Justice, Defense, and Homeland Security, and the Federal Trade Commission, on security-related issues. He serves on the Executive Committee of USACM, the U.S. public policy committee of ACM, the leading professional society for computer scientists. In 2003, Scientific American magazine named him to its list of fifty global leaders in science and technology.

The CHAIRMAN. Our second witness is Gary Smith. Mr. Smith is the election director in Forsyth County, Georgia. Georgia uses a paperless DRE system statewide, and for those who don't know what DRE stands for it is direct recording electronic computer. Basically it is a type of computer we have displayed here.

Mr. Smith uses a Diebold system that was the subject of the Princeton study. Mr. Smith also participated in the recount of the Cuyahoga County primary conducted on a DRE system with a paper audit trail. Mr. Smith, you are recognized.

STATEMENT OF GARY SMITH, ELECTION DIRECTOR, FORSYTH COUNTY, GA

Mr. SMITH. Well, as was mentioned, my name is Gary Smith, I reside——

The CHAIRMAN. Is your microphone on?

Mr. SMITH. My name is Gary Smith and, as you mentioned, I am the election director for Forsyth County, Georgia, a county just north of Atlanta. It is quite a fast-growing county. We have about 80,000 registered voters and we are one of the top fastest-growing counties in the United States, so we have a lot of issues that we have to deal with all the time.

One of the things I think that is important maybe is to look at what those of us as election directors—how we come about. I am actually appointed through a selection committee that comes about where a grand jury is brought forth, they pick a panel of people who have the background to be able to do this. It is then sent up to the chief superior court judge and then I am selected from that. I was selected from that process.

I am in my second term as the director of elections. It is a term of 4 years, and it is a nonpartisan position. Prior to coming into this position I spent most of my time working in the private sector. I retired. I was running various companies, and I have worked most of my life in industrial automation. So I have a technical background. I have an undergraduate degree in electrical engineering and I am a certified election registration administrator from a program administered by Auburn University.

As a director of elections, one of the things that I have been privileged to do is to sit on a task force, several of them. One has been from the Georgia task force, which allows me to be able to participate and look at new processes and equipment that we apply to elections in our county and State. In addition to that, I served on a national task force for election reform for 2004 where we looked at all the processes across the country with regards to elections. In addition, I think you just mentioned I did lead the manual recount for the Cuyahoga County VVPAT so I have some practical experience with that and I was happy to be able to do that. I spent a week at it, as a matter of fact.

We have implemented the DREs. The one that you are looking at right here, which is the Diebold-TS unit, my county and 158 counties in Georgia implemented this during the general election of 2002. We have held, from what I heard was the last count, something like 2,500 elections in our State. In addition to that I have held elections on special elections, primaries, general elections,

run-offs and just about any kind of election, and a municipal election as well. So, again, we have a lot of experience with them.

One of the things that I think has been talked about a lot and I think we have to deal with is how do you look at the security and integrity of this kind of equipment. It starts, obviously, with the vendor who builds the equipment, goes through the independent testing laboratories that then look at it to make sure what we are receiving has the technical wherewithal to be able to provide us with a piece of equipment that really meets what our needs are. Thirdly, we have in our State, which I am very proud to talk about, the Center for Election Systems, a program administered by Kennesaw State University and Dr. Britt Williams, a well-known authority in elections.

We do all of our creation of our ballot cards and that sort of thing through this group, and so it is another level of testing that we have that goes on.

Lastly, it is up to those of us who are election directors to hold these elections, so I am tasked with a lot of the things that Mr. Felten has talked about, which is maintain the security and integrity of the process that goes on with elections. I guess we are where the rubber meets the road as much as anything.

So that is our job. I am not going to go through all the details with regards to certification because it is certainly going to take a lot more than a few minutes, but it is in my paper and I hope that you will look at it. I think where we pick it up is where we pick up the memory cards, as Mr. Felten has mentioned, that come to us from the Center for Election Systems, the process of making sure that they come to us under the chain of custody manners, that we know that there is at least more than one person that has access to what we are talking about and they are looking at.

We go through a process called logic and accuracy testing. This is when the process that he has talked about goes through the first part, where we are taking the memory cards, we are marrying them essentially to the voting machine, and then we are taking them through the testing process, at which time then we lock the machines up and we pass them on to the next level, which really is the election poll worker himself.

And what I would like to do is to show you some of the chain-of-custody forms and I think they are in front of you too. If they are not, I am going to show you one actually that is going to be—okay. It is as good as it can get up there but I think most of you can probably see it.

What I am pointing out in it—is it okay if I stand up?

The CHAIRMAN. As long as you carry the microphone with you so all the people in the overflow room can hear you too.

Mr. SMITH. Can you hear me now?

The CHAIRMAN. Yes.

Mr. SMITH. All right. I think what is critical about this, I think this is one of the things maybe that because we are doing it statewide, we have an awful lot of good chances to be able to work the processes out. And I think Mr. Felten, one of the things he said is you need to have good chain of custody in these things. This actually is for the precinct Big Creek. This is actually an actual form that we are using. It says here item number 1, custodian certifi-

cation form for the AccuVote-TS units that are going to be used. Under point number 2 what I have got here is the touch screen serial number, which has not got a number in here, 116827.

Then across here what you are looking at is all of the tests that we take individually to run on the machines. This takes about 15 minutes per machine to run. It is a process that is done under my direction, and we actually have done this for 500 machines for the upcoming election.

The next point that is important to look at is there is a seal number that is right here. That seal number, what I am going to show you is how it is carried forward to the process where when we are holding the election at the precinct, what happens with it. This machine then is sealed up, it has a wire serial number on it. So there is no access to this machine once the logic and accuracy test is done.

Now, the next form I am going to show you is right here. This is a form then that is carried forward to the precinct itself so that when the poll workers, poll manager and his assistant, this is their responsibility; this is a form that is signed in triplicate, one goes to the Secretary of State, one goes to me and one goes to the clerk of the superior court. You will notice again it is for precinct Big Creek 01. This is the recap sheet that goes with it. Here again is the serial number. If we had looked back before, we would find that that serial number is the same one as here.

Here is the serial number that then shows up on—that is transferred from the original L&A testing. Now what happens with it is we open up the machines, we go through it, we do the count number, and then at the end of the election, because this is the recap sheet, the key part here is that there is another mechanical low-tech seal put on it. It is a wired seal so it is kept on there all the time.

That is the process that we go through. I wanted you to be able to see that.

The CHAIRMAN. I am going to have to ask you to wrap up because we have a lot of witnesses and a lot of discussion.

Mr. SMITH. Okay. I am sorry.

The CHAIRMAN. Is that it?

Mr. SMITH. The other part I wanted to talk about, and I think this has to do with the comments that Ms. Millender-McDonald said, is what is the confidence that people have in it. I would like to at least respond to that at another time, because we have done surveys in our county, too, which show that 99 percent of the people feel that the process is an excellent process. So there is a high level of confidence in our equipment.

The CHAIRMAN. All right. We can defer that to the question period.

Mr. SMITH. Thank you very much.

The CHAIRMAN. Thank you.

[The statement of Mr. Smith follows:]

Testimony of Gary J. Smith
Director of Elections
Forsyth County, Georgia
Before the Committee on House Administration hearing on
Electronic Voting Machines: Verification, Security, and Paper Trails
September 28, 2006

Mr. Chairman: My name is Gary Smith and I have been the Director of Elections for Forsyth County Georgia for the past 4 ½ years. I am an appointed official and am selected by a Grand Jury with recommendations to the Senior Superior Court Judge. It is a non-partisan position.

Prior to becoming Director of Elections, I served in many positions within the private sector with emphasis on industrial automation. My undergraduate degree is in electrical engineering from the University of Illinois and I am a Certified Election and Registration Administrator.

As Director of Elections, I have also been privileged to serve on several committees that have given me an opportunity to see elections not only on a local and statewide basis, but from a national perspective as well. Within our State of Georgia, I am a current member of the Georgia Task Force for Elections–which reviews new processes and technology that will be implemented and I have held statewide offices for both our Georgia Election Officials as well as the Voter Registrars Association of Georgia. From a national perspective; I served on the National Task Force on Election Reform for 2004 and have hosted other statewide groups that have come to Georgia to view operational procedures with the use of Direct Recording Electronic (DRE) voting systems. In addition, I led the manual recount of the Cuyahoga County Ohio Primary Election for Election Science Institute.

We implemented Diebold's AccuVote TS DREs in our county along with the other 158 counties in Georgia during the General Election of 2002 and have experience in all types of elections i.e. Municipal, Special, Primary, General and Run-offs. We believe this experience allows us to speak with some authority on the process of elections held using DREs.

During this period of elections, we have worked very closely with the Secretary of State's office and our designated Center for Election Systems – Kennesaw State University (KSU). KSU has helped to develop the security features that we believe allow us to provide a safe and secure election.

Within the State of Georgia, the organizations involved in assuring system integrity are:

- Election System Vendor – Diebold
- Qualified Federal Testing Laboratory (ITA)
- Kennesaw State University – Center for Election Systems
- County Election Officials – i.e. Forsyth County Board of Elections

What are the responsibilities of the individual organizations?

Election System Vendor - Diebold

- Designs and builds the Election System
- Submits the Election System to the ITA to verify compliance with Federal Voting System Standards
- Adheres to State level Certification tests
- Completes Federal and State testing and receiving approval ships systems to the counties

Qualified Federal Testing Laboratory - ITA

- Reviews the System for compliance with the Federal Voting System Standards
- Issues Certification Report on Complete System
- Submits the Certified System to the KSU Center for Election Systems where State Certification tests are performed

KSU Center for Election Systems

- Reviews the System for compliance with State of Georgia Election Code and Rules
- Tests the System for the presence of any unauthorized/fraudulent code
- Develops a validation program used to test the System installed in the counties
- Verifies that the System installed by the vendor in the county is identical to the system received from the ITA and certified by the KSU Center for Election Systems

County Election Official – Forsyth County

- We maintain, store and protect the System through the use of various chain of custody procedures and physical security features which include

but are not limited to storage under security cameras, computer coded access, locked equipment storage, hardwired security tags, no access to the internet etc.

- We use the System in accordance with Georgia Laws and Rules to conduct elections.

Security is viewed in three different layers, all working together to maintain the system integrity.

The first layer is software security, consisting of the normal elements of user ID's, unique passwords, and audit trails of all activities performed on the systems.

The second layer is procedural security. This includes the four levels of testing:

- **Certification Testing on the National Level**
  - These are nationally prescribed tests outlined by the FEC and are performed by Independent Testing Authorities that have been approved by National Association of State Election Directors (NASED).
  - The Independent Testing Authorities (ITAs) review the software and hardware to make sure the system meets the stringent guidelines for election equipment.
  - Part of the tests performed is an analysis of the election system's source code to ensure that there is not fraudulent code embedded within the system.
  - Any voting system must pass these rigid and extensive tests before even being considered for any use in Georgia.
  - If any changes occur to the election system's components, the system must be sent through qualification testing again.

- **Certification Testing on the State Level**
  - These tests are designed to ensure the election system performs the duties required by Georgia Law, Georgia's State Election Board's Rules and Regulations, and Rules of the Secretary of State.
  - Tests are performed on an exact copy of the system certified by the ITAs. The ITAs forward an exact copy of the national certified system to the State for testing. This ensures that the system tested by the State is identical to what was submitted to the ITAs by the election system manufacturer. This ensures that the Vendor does not make unknown changes to the certified system after national tests are completed and before state test begin.
  - The test performed by the State mirrors actual election conditions faced by election systems in real use.
  - To make sure the software running the election system is free of hidden or fraudulent code, the systems clocks are moved forward to an actual election date. Once the clocks have been changed the

simulations are then run. The movement of the clocks is designed to uncover hidden code that only becomes active on election dates.

- The tests performed are carefully scripted and conducted under constant supervision. The State level tests are performed by the Center of Election Systems at Kennesaw State University and is overseen by Dr. Brit Williams; a member of the NASED technical board which approves ITAs for service in the qualification testing on the national level.
- The system is put through stress tests to uncover the true capacity of the system and to ensure the system continues to record, store, and process data correctly even under extreme conditions.
- Once the system has cleared certification testing, an electronic signature is taken of the certified system. This electronic signature is then used to verify systems once they are installed in local county election offices. If a system is installed in a county and its signature does not match the signature of the certified system, then that system cannot be used. In addition, this system check can be run at anytime, even during the election process if necessary.

- **Acceptance Testing**
  - Performs physical and functional testing of each unit that has been purchased, repaired, or upgraded
  - Verifies the system installed by the Vendor matches the system certified for use in Georgia.
  - Tests the functionality of the entire system as well, to make sure the system continues to function as shown during the certification tests.

- **Logic and Accuracy Testing**
  - Verifies again that the system is functioning in a manner consistent with certification test results.
  - Election data to be used in an actual election is loaded to the voting system and the system is tested to ensure the choices entered by voters are recorded in the system as intended.
  - Every voting machine to be used in an election must pass this process before it can be used in an election.
  - This process is conducted in public view.
  - Records are kept by local election officials verifying that each machine has been tested and has been found to be functioning properly.
  - At the conclusion of this testing, the units are closed and sealed and are not opened again until the morning of the election.

Access to the election equipment is tightly controlled, including documentation of who, what, when, and why access is granted.

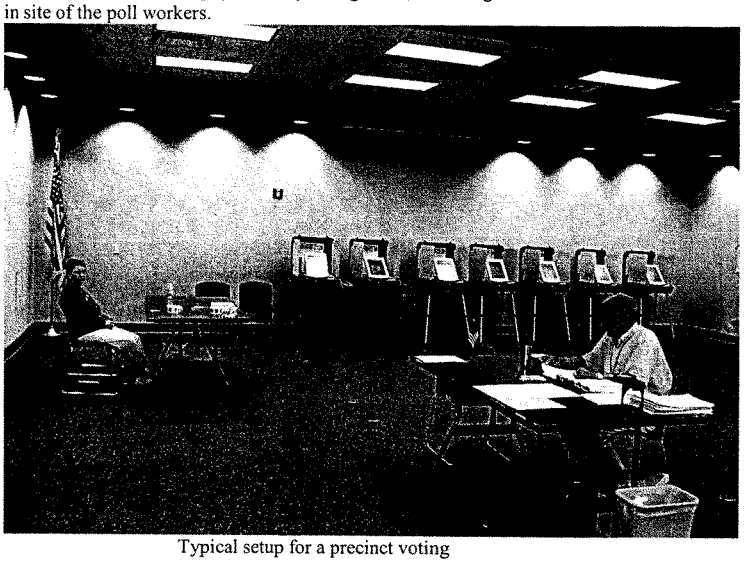
Voters must proceed through a check-in process at the polls or the absentee precinct prior to being given access to the voting units.

Voter access cards do not leave the confinements of the precincts during the voting period. This is assured by requiring each person leaving the polls to give up their access card at the exit station.

All tests run prior to the opening of polls on the morning of an election are done in public view and are done by a team of poll workers. A single poll worker does not perform tests on the voting system without assistance from at least one other poll worker.

Periodically through the voting day and at the close of polls, the numbered list of voters, voter's certificates, and elector's list are reconciled with the number of ballots recorded by the voting units. This is done to ensure the system has not recorded more votes than voters voting. All reconciliation sheets are signed in triplicate.

Poll workers patrol the voting area throughout the day to ensure voters are not tampering with the voting system. By Georgia law, all voting booths must be in site of the poll workers.



Typical setup for a precinct voting

Voting units are placed in a way that poll workers and the public can view the actions being taken in the voting booths without endangering the secrecy of the voter's voted ballot.

Multiple poll workers perform Poll closing procedures. A single poll worker does not perform closing procedures on the voting system (i.e., printing of tally tapes from voting units) without assistance from at least one other poll worker.

All sensitive materials maintained in the polling precinct are kept in sealed containers i.e. the supervisor card used to close out the election.

All compartments of the voting units are locked, with only the poll manager having access to the keys that unlock them. The comment from the Princeton report has changed the way that we will lock up our voting units after they are started up during the election – we are going to add on a security tape similar to that shown below. Although ours will have a digital seal and will be recorded for purposes of security. We think this is a positive action.



Security Seal on DRE access to memory card

A parallel monitoring test is performed for each statewide election with six counties being randomly selected. For each of these counties, a precinct is randomly selected. The actual ballot styles for this precinct are loaded on a voting unit at the Center for Election Systems. At Approximately 10:00 am on Election Day, a pre-defined script is voted on each of the six machines. Upon completion of the voting, the election on each machine is ended and a result tape is printed. The count on the result tape is compared to the script count for each race in that precinct. For at least one precinct, the actual ballots cast are printed and compared to script to verify that the votes are recorded properly.

The second phase of the parallel monitoring test consists of randomly selecting at least three counties and a precinct for each county. On election night, the counties make copies of the result tapes for all of the voting units in the selected precinct and mail them to the Center for Election Systems. Once the certified results have sent to the State Elections Division, a copy of the CD for each of the three counties is obtained. The actual ballot images for at least two machines in each precinct are printed. The ballots are manually counted for the top two races. The manual count is compared to the count produced on election night on the result tapes for the selected units.

The third level of security deals with physical security and includes the following:

- **Source code is escrowed**
  If questions were to arise about the software in use, the escrowed source code could be used to verify whether or not the system in use had been tampered with or not.

- **Secure Storage of Voting System and components**
  - Voting units used to collect votes are stored in secure areas under the direction of each county election superintendent. Access is limited to employees of the county election office.
  - The election management system used to create the various ballots necessary for an election, and used to program the voting units for elections is stored on a dedicated computer that is not connected in any way to any other internal or external network.
  - Access to the computer is limited to county election officials, or their designees.
  - The dedicated computer storing election data contains software only approved by the Secretary of State.
  - When not in use, the voting units are stored in a protected area and the dedicated election management computer is locked.
  - All components of the voting system, when not in use, are stored in a secure location by the county election superintendent.
  - During an election, units are sealed prior to being delivered to precincts. These seals are recorded and monitored.
  - At the conclusion of an election, the removable memory from each unit is removed and placed in a sealed container and returned to the county election office for tabulation.
  - In addition, the voting units themselves with their internal backup memory are sealed and returned to the secured storage facility.

Protecting System Integrity

Three distinct functions are performed to protect the integrity of the System:

Verify the System at Receipt (State Certification Test by KSU)

- Using the System as delivered from the ITA, set up and conduct sample elections with known outcomes that are representative of Georgia general and primary elections.
- Conduct high-volume tests to determine capacity limits of the System
- Conduct tests to determine the System's ability to recover from various types of errors

Verify the System at Installation

- KSU ensures that the System installed in the county is identical to the System received from the ITA and certified by the State
- KSU prepares a validation program that will detect any changes to the System installed in our county
- KSU runs the validation program against the System installed in our county (after vendor installation)

Verify the System is Performing Properly (Forsyth County)

- Logic and Accuracy Tests are performed prior to each election
- Performance of all System components is verified
- Specific ballot information for each memory card in each precinct is verified
- Touch screen units are set for election, locked and sealed with a hard wired numerical seal
- Our server is always kept in a secured location behind three computed coded solid doors and a security camera
- No extraneous software is installed on our server
- There is no network connectivity
- Physical access is limited to authorized personnel
- Touch screen units are protected by layers of physical security prior to Logic and Accuracy and afterwards with digital access, security cameras and hardwired serial tags.
- Touch screen units that are used for elections are secured and locked when not in use

Validation Program (Hash Codes run by KSU during testing and on request

- Based on NIST standards contained in FIPS 180-2, established in August 2002
- Run 'Hash' on the System certified by KSU's Center for Election Systems. This creates File 1.

- Run 'hash-cmp' to compare File 1 with a new 'hash' on the System in the County
- They must be identical

In the most recent report from Princeton University among their findings are issues that deal with the security of DRE systems. We believe that we have mitigated many of these problems through the use of the processes above. Specifically there would be problems if as the professors pointed out, that poll workers or others would have unsupervised access to the machines – in our county, poll workers and others do not have unsupervised access to a voting machine or memory card. It is not a practice in Forsyth County to allow any poll worker unsupervised access to the machines.

The DREs in Forsyth County and Georgia are never networked together minimizing the risk of any spreading of viruses. In addition, KSU has provided us with "sanitized" memory cards to minimize the risks of obtaining a voting machine virus. All memory cards in Georgia were returned to KSU for the process and returned to us after they had been cleaned – this is another example of the lengths that we go to in insuring a virus free environment.

Many "white papers" have been written both pro and con with respect to the use of DREs and especially with regard to the ones that have been implemented in Georgia. Our own Secretary of State – Cathy Cox has said that *"Due to the built-in redundancy, we know that, after more than 3,000 elections, not one vote has been lost due to any type of equipment malfunction."*

Ultimately, it is about the confidence that people have in the voting process itself that is important. The first major study that was done by a public institution about the state of voting in Georgia was done by the University of Georgia's Carl Vinson Institute of Government and is included below for your benefit.

GEORGIANS FAVOR ELECTRONIC VOTING

ATHENS, GA – Georgians overwhelmingly prefer electronic voting to other methods of voting, according to the most recent Peach State Poll. Seventy percent of the voting age public say they are more comfortable casting their respective ballots electronically on the touch screen machines than by punch cards (preferred by 8 percent) or by marking paper ballots (12 percent). Eighty-four percent of Georgians say that the touch screen voting machines are an improvement over using punch cards, and 82 percent say they are an improvement over paper ballots on which voters mark with a pen.

In addition, poll respondents express a high level of support for a uniform voting system. The Peach State Poll, a quarterly survey of public opinion conducted by the University of

Georgia's Carl Vinson Institute of Government, finds that 95 percent of the public believe that having a uniform system is either very important (77 percent) or somewhat important (18 percent). Only 17 percent of Georgians believe that individual counties should be allowed to decide the method by which their constituents cast votes.

Other Peach State Poll results:

- A plurality of Georgians say that the greatest advantage of the new fully electronic voting system is that it is convenient to use (44 percent); 22 percent cited increased accuracy as the greatest advantage.

- When asked what they believed to be the greatest problem with the new voting machines, a plurality (26 percent) said that there were no problems, and 19 percent cited the likelihood that some people are not comfortable with new technology as the greatest problem.

- Georgians with higher levels of education are more likely to believe that the new electronic voting system will increase the accuracy of Georgia's elections. While 56 percent of those with a high school education or less believe that the new system will improve the overall accuracy, 73 percent of those with postgraduate education believe it will.

- While 70 percent of the public say they are most comfortable voting on touch screen machines as opposed to punch cards or other paper ballots, that percentage drops to 58 percent for Georgians over age 65.

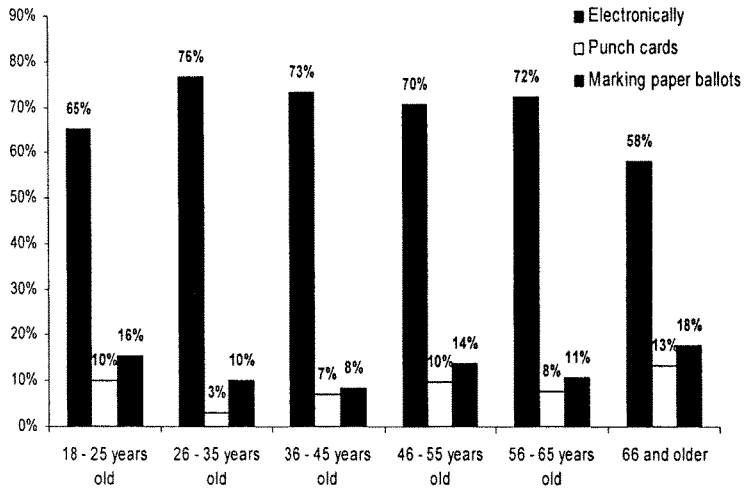
- Georgians who do not use automatic teller banking machines report being less comfortable and more skeptical of the electronic voting machines than are those who use ATMs. Still, a majority (55 percent) of those who do not use ATMs show more comfort with the electronic voting machines than with any of the alternatives.

These data were taken from a Peach State Poll survey conducted between November 16 and November 23, 2003. The poll included 807 telephone interviews of randomly selected adults in Georgia. For a sample of this size, the margin of error at the 95 percent confidence level is +/-3.5 percent.

The Carl Vinson Institute of Government, a public service and outreach unit of the University of Georgia, has as part of its mission to provide policymakers with systematic, objective research to inform policy decisions. In accordance with that mission, the Peach State Poll aims to give voice to the public on important policy matters and issues pertaining to political, social, and economic life in Georgia.

For more information on this survey or other Peach State Poll results, see www.vinsoninstitute.org/peachpoll.

Comfort level with various methods of voting by age

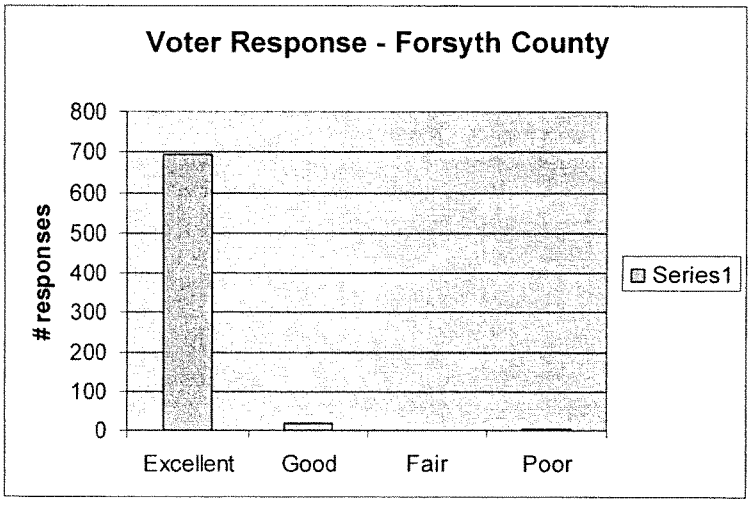


FORSYTH COUNTY VOTERS LIKE ELECTRONIC VOTING

In our own way in Forsyth County, we have tried to track the issues and concerns that our voters have in order for them to have a better election day experience. To do this, we have a response card that is randomly handed out to voters in our precincts – it includes the following questions:

- How was the service
- How can we improve
- Additional comments
- Name/Address optional
- Precinct #
- Date

We have analyzed the first 715 responses and they are attached for your benefit. Of the responses the following information is available:

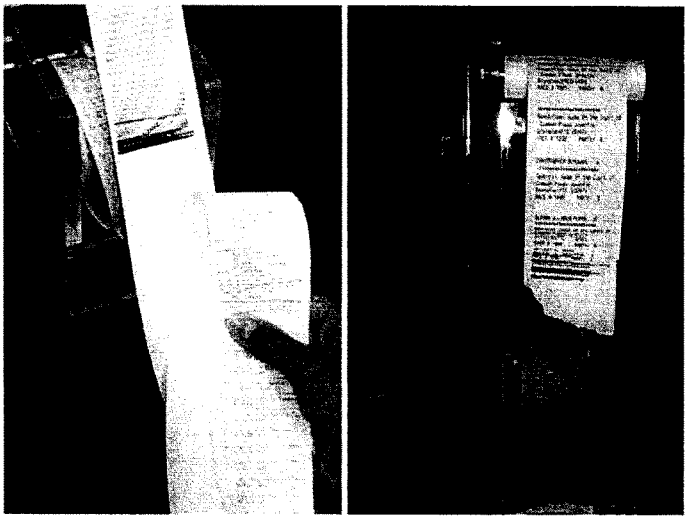


The above response is an indication of the entire experience that our voters have had with the entire process of an election. You are able to see from their attached comments that they are very pleased with the process and only a few (less that 0.0002) of the voters have asked for a VVPAT. The voters have certainly expressed a lot of opinions and we routinely meet to be able to improve our operations.

A significant amount of this positive experience goes to the excellent poll workers we have in our county. Poll workers in Forsyth County go through a selection process that includes a personal interview with me or my Outreach Coordinator. In addition, every poll worker is required to attend training prior to each and every election. The minimum period for a training session is three hours and includes both small classroom sessions and hands on portion. All poll workers will train together with their precinct so that they are all knowledgeable of the interaction that goes on during Election Day. We also grade our poll workers and provide additional training for those who do not meet minimal standards.

In June, I was asked by Election Science Institute to lead the manual recount of the Cuyahoga County Primary Election of 2006. This study is well documented in the report written by ESI and reflects the problems associated with having a paper document VVPAT used as the legal ballot during an election. As it was pointed out by Princeton, a denial of service could easily be implemented when the legal ballot is the VVPAT. During our recount of the VVPAT, it was evident that the voters were not paying attention to the VVPAT as they would have certainly not continued to cast their ballots when the printed tape was either not indexing, was missing or blank – all of these issues were found to be in existence.

I have attached below photos of issues with the VVPAT:



It is my hope that the energy and talent expressed by the academics that have researched exhaustively the inter workings of the aforementioned DRE in their Princeton report could provide a solution that is easier to implement than the VVPAT. Possibly, it could be along the lines of that suggested by election administrators in the National Task Force on Election Reform that is not limited to paper:

> "That guidelines be developed by the National Institute of Standards and Technology (NIST), through the EAC, for a scientifically sound, independently verifiable audit trail for direct record electronic (DRE) voting systems and that such guidelines not be restricted to contemporaneous paper replica but also include guidelines for electronic, audio, video or other media to provide verification of the integrity of recording and tabulating votes.
> 22. That, for DRE voting systems, guidelines be developed by NIST, through the EAC, for the contemporaneous recording of each ballot record, on a secure medium, to provide a redundant record"

While costs are not necessarily the overriding factor in purchasing or changing voting equipment they can not be ignored. Our voters in Forsyth County have invested almost an incremental $1,000,000 over the cost of the systems given to us by the State of Georgia in additional equipment and training over the past four years. We certainly can not be

expected to continue this type of investment or make changes, when the equipment still has at least 70% of its expected life cycle to be used.

In conclusion, we believe that the voters in Forsyth County Georgia have spoken positively that they have a voting system that has provided them with the assurances that their votes are being counted and tallied correctly.

Thank you for the opportunity to share my thoughts and experiences with you.

Acknowledgements: I would like to thank Ray Cobb and the KSU Center for Election Systems for their assistance, technical help, information and feedback. Georgia is fortunate to have such an institution as our independent and capable entity responsible for testing and certification of election equipment.

Attachments: Voter Responses Forsyth County Georgia

The CHAIRMAN. As a reminder to those, I should have mentioned it before, you have the little device in front of you with the lights on it. Green means go, yellow means sum up, red means you are in deep trouble. So please keep an eye on the clock.

Next I am pleased to recognize Ms. Barbara Simons, past president of the Association for Computing Machinery, and she has done a lot of work on voting systems. Dr. Simons, you are recognized.

STATEMENT OF BARBARA SIMONS, MEMBER, U.S. PUBLIC POLICY COMMITTEE, ASSOCIATION FOR COMPUTING MACHINERY

Ms. SIMONS. Good morning, Mr. Chairman, members of the committee. On behalf of the computing professionals that constitute the Association for Computing Machinery I want to thank you for the opportunity to testify today about e-voting system security and the need for voter-verified paper trails. Secure, reliable, usable and accessible voting systems are critical toward assuring transparent, fair and inclusive elections. These are not mutually exclusive goals. I shall discuss aspects of both security and accessibility this morning.

First, security. Because of the risks of software bugs, malicious code or computer failure, we cannot trust that the results in a paperless voting machine accurately reflect the will of the voters. That is why voter-verified paper ballots or audit trails (VVPATs, as we refer to them) are needed. VVPATs are automatically produced by an optical scan system, since the ballot is verified by the voter. Fortunately, 48 percent of counties have optical scan systems so they already have VVPATs.

Optical scans can be used together with tactile ballot sleeves or accessible marking devices for accessibility. Some DREs have been retrofitted to produce VVPATs; in fact, all of them for use in California, as Congresswoman Lofgren said.

Two years ago ACM, a leading computer society, issued a statement calling for well-engineered voting machines that allow every voter to verify his or her record has been accurately cast by the inspection of a physical (e.g. paper) record.

At its 2006 national convention, the League of Women Voters passed a resolution calling for voter-verified paper ballots or records to be used for audits and recounts. The League also urged that routine random audits be conducted in every election.

Both the ACM statement and the League's resolution can be found in my written testimony.

In summary, as a defense against malicious or buggy software we must have: reliable, well-engineered VVPATs, policies and procedures that guarantee the integrity of the paper records; security storage and delivery of machines and so on, mandatory random manual audits of VVPATs; and a full manual recount if discrepancies are uncovered, unless there is evidence that the VVPATs have been compromised.

I will now discuss accessibility.

People with disabilities should be able to vote privately and independently and be able to verify their votes.

HAVA does not require the DREs be used for accessibility. There is evidence that a number of people with disabilities are finding that DREs are not meeting their accessibility needs.

Kelly Pierce, a nationally known advocate for the blind and visually impaired, reviewed tactically discernable controls, spoken prompts, visual display, poll worker assistance, volume control and normalization, and ballot review for four voting machines. In his report for Cook County State Attorney's Office, Pierce concluded that if any one of the four machines were to be deployed in Chicago or suburban Cook County, many voters with disabilities, particularly blind voters, would not be able to cast a ballot independently and privately.

Blind computer scientist Noel Runyan discussed his frustration with his hour-long voting experience in the 2004 Presidential election, and I quote: It took me 30 minutes to work my way through the ballots and make my selection. After that I had quite a bit of trouble getting into the review mode to get a full list of all my selections. When I did, it went on and on for 23 minutes, like a long uncontrolled drink from a firehose. The review function read each item and then at the very end said my selection was for that item. It even threw in details of what the fiscal impact would be and took forever.

"This is completely backwards."

He went on to say: "From the time I signed in and got my voter smart card, it took 8 minutes to reboot the audio voting machine; 30 minutes to make my choices; 23 minutes to review and verify; and another 4 minutes to make a correction and record my vote. Not counting the hour waiting in line, it took me about 65 minutes to mark and record my ballot."

We do not have to settle for inaccessible voting systems. Old technologies such as text to audio devices, tactile ballot sleeves, and ballot market and generating systems could be combined with new technologies that make the entire voting and verification process accessible, while remaining auditable.

Technology, if engineered and tested carefully and if deployed with safeguards against failure, can reduce error rate, provide more accessibility, increase accountability and strengthen our voting system. However, the current state of e-voting technology leaves us far short of these goals. We need paper trails and manual audits to protect us against failures and attacks. We need additional research to make voting machines more usable, secure and accessible. And we need to work together to achieve these goals. Thank you.

The CHAIRMAN. Thank you very much.

[The statement of Ms. Simons follows:]

Statement of Barbara Simons for the Committee on House Administration Hearing on Electronic Voting Machines
September 28, 2006

My name is Barbara Simons. I am retired from IBM, where I was a Research Staff Member at the IBM Almaden Research Center for many years. I have been working almost exclusively on voting technology issues since 2000, when I was a member of the National Workshop on Internet Voting. The workshop, convened at the request of President Clinton, produced a report in 2001 in which we strongly recommended against Internet Voting. I also participated on the Security Peer Review Group for the US Department of Defense's Internet voting project (SERVE) and co-authored the report that led to the cancellation of SERVE because of security concerns. More recently I co-chaired the Association for Computing Machinery (ACM) study of statewide databases of registered voters. I am also co-authoring with Professor Doug Jones a book on voting machines to be published in 2007 by PoliPoint.

I was President of ACM from July 1998 until June 2000. ACM is the oldest and largest scientific and educational society of computer professionals, with approximately 80,000 members. I founded ACM's US Public Policy Committee (USACM) in 1993 and have served for many years as the Chair or co-Chair of USACM.

We must make our elections more secure, reliable, accessible, and verifiable.

We all want elections that are reliable, secure, accessible, and trusted by the public. Given known security risks, the possibility that software bugs could generate incorrect election results, or that computerized voting machines may fail during an election, we cannot trust that the results recorded in a paperless voting machine accurately reflect the will of the voters. Providing a voter verified paper trail is a significant step toward mitigating these risks, restoring transparency to the election, and ensuring the public's trust.

Because paperless Direct Recording Electronic (DRE) devices cannot be audited, many states have mandated that DREs produce a voter verified paper audit trail (VVPAT) or voter verified paper ballot (VVPB). We have seen that careful and well engineered implementation of this requirement is critical. Some of the most widely used DREs have retrofitted their machines by adding reel-to-reel thermal printers. Unfortunately, there have been a number of problems with these continuous roll printers, including jamming, privacy concerns, and difficulties conducting a manual count of the paper.

There are high quality printers that are much more reliable, that produce easy to read text, and that could print VVPBs that are easy to count manually. Our voting systems should not depend on mediocre equipment.

Precinct based optical scan voting systems also produce VVPBs, since by definition the optical scan ballot is verified by the voter when he or she marks the ballot. Accessible

optical scan ballots can be produced using tactile ballots or electronic ballot marking systems. Optical scan ballots can be manually counted and used to audit elections.

As a defense against malicious or buggy software, we must have:

- reliable, well engineered, accessible VVPBs;
- policies and procedures that guarantee the integrity of the paper, control of custody, legibility, etc.; and
- routine mandated random manual audits of the VVPBs that instill voter confidence and that verify the accuracy of elections.

If the manual count does not match the count produced by an optical scan system or by a DRE, then all of the paper ballots must be manually counted in an open and transparent fashion. Unless there is evidence that the VVPBs have been compromised, the paper ballots should be used to determine the election results.

We can consider alternatives, such as cryptographic based systems, if and when voting technology is commercially available that is demonstrably secure, reliable, easy to use, accessible, believable, and understandable to the average voter.

Most computer professionals oppose paperless voting machines.

Computer scientists have been generally skeptical about computerized voting machines, because we know that they are not transparent. You cannot simply look inside a machine and clearly see if it is performing in a trustworthy manner. Computerized voting has a lot of advantages, but all computerized voting systems currently available carry risks. We recommend VVPATs or VVPBs not to eliminate fraud, but rather to increase the safety of voting systems and to allow for routine election audits.

Two years ago ACM issued the following statement[1] calling for well engineered voting machines that provide every voter with the ability to verify that his or her vote has been accurately cast by inspecting a physical (e.g. paper) record.

ACM Statement on E-voting

Virtually all voting systems in use today (punch-cards, lever machines, hand counted paper ballots, etc.) are subject to fraud and error, including electronic voting systems, which are not without their own risks and vulnerabilities. In particular, many electronic voting systems have been evaluated by independent, generally-recognized experts and have been found to be poorly designed; developed using inferior software engineering processes; designed without (or with very limited) external audit capabilities; intended for operation without obvious protective measures; and deployed without rigorous, scientifically-designed testing.

To protect the accuracy and impartiality of the electoral process, ACM recommends that all voting systems – particularly computer-based electronic voting systems – embody careful engineering, strong safeguards, and rigorous testing in both their design and

operation. In addition, voting systems should enable each voter to inspect a physical (e.g., paper) record to verify that his or her vote has been accurately cast and to serve as an independent check on the result produced and stored by the system. Making those records permanent (i.e., not based solely in computer memory) provides a means by which an accurate recount may be conducted. Ensuring the reliability, security, and verifiability of public elections is fundamental to a stable democracy. Convenience and speed of vote counting are no substitute for accuracy of results and trust in the process by the electorate.

The League of Women Voters' resolution on voting systems.

In addition to the technical community, good government organizations have expressed concerns about the security of paperless voting machines. For example, at its 2006 national convention the League of Women Voters passed a resolution on voting machines calling for a voter verified paper ballot or record that would be used for audits and recounts. The League also urged that routine random audits of these paper ballots/records be conducted in every election. Here is the resolution[2]:

Whereas: Some LWVs have had difficulty applying the SARA Resolution (Secure, Accurate, Recountable and Accessible) passed at the last Convention, and
Whereas: Paperless electronic voting systems are not inherently secure, can malfunction, and do not provide a recountable audit trail,
Therefore be it resolved that:
The position on the Citizens' Right to Vote be interpreted to affirm that LWVUS supports only voting systems that are designed so that:

1. they employ a voter-verifiable paper ballot or other paper record, said paper being the official record of the voter's intent; and
2. the voter can verify, either by eye or with the aid of suitable devices for those who have impaired vision, that the paper ballot/record accurately reflects his or her intent; and
3. such verification takes place while the voter is still in the process of voting; and
4. the paper ballot/record is used for audits and recounts; and
5. the vote totals can be verified by an independent hand count of the paper ballot/record; and
6. routine audits of the paper ballot/record in randomly selected precincts can be conducted in every election, and the results published by the jurisdiction.

Insecure storage and handling of voting machines.

Professor Ed Felten, who is testifying today, recently released a very important study of fundamental security vulnerabilities of Diebold TS machines. The study illustrated how having physical access to one of the machines for even a minute was sufficient to allow a malicious individual to install fraudulent software.

There already has been a fair amount of press about the risks of voting machine "sleep-overs." This practice involves having a poll worker take a machine home prior to the election and bringing it in on Election Day. Decentralizing the physical security of machines significantly increases the number of people with access to a machine before an election. But even if machines are not delivered to poll workers' homes, there still can be significant security threats stemming from pre-election deliveries of machines, as I observed while serving as a Santa Clara County polling station inspector in the November 2004 election.

The county delivered five paperless DREs to our polling station – a commons room in a Stanford University dorm – about a week before Election Day. When the woman who made the space available for the election arrived at work, she moved the machines from the insecure commons room into her office, where they remained under lock and key until the night before the election.

My fellow poll workers and I set up the voting machines in the public commons room the night before the election so that the batteries could be fully charged. For the rest of the night the machines remained unattended.

When initially delivered, the machines were "protected" by two levels of numbered tamper evident tape. The first level was removed the night before the election, when we did the initial set-up. The second level was removed on Election Day. All of the removed tapes were included in the material that we returned to the county election officials.

I had no idea before the election as to what the tamper evident tape should look like, because I had never seen any. Even if I had been shown a tape, without additional training I doubt that my memory would have been adequate for me to know if a counterfeit tape had been used.

Security risks of the procedures deployed by Santa Clara County.

There are multiple security risks, depending on the goal of the attacker. Here are a few:

1. Hacking the voting machine software without being detected. This could have been done either by someone who had access to the machines while in the commons room, or by someone who had access to the office where the machines were stored. To avoid detection with certainty, it would have been necessary to acquire identically numbered tamper evident tape, for example by ordering it on the Internet or obtaining it from an insider working for the county.
2. Hacking the voting machine software and risking detection. Since we poll workers had never seen the tamper evident tape and had no idea of what the numbers on the pieces of tape should be, we would not have been able to determine that someone had hacked the software and replaced the original tapes with different tamper evident tapes. Such an attack might have been detected by election officials if they had reviewed the tapes that we returned. However, since

the election would have been over, it's not clear what election officials would have done. Furthermore, if the attacker had acquired identical or nearly identical tape and used the numbers from the original tapes on the counterfeit tapes, it's likely that even diligent election officials would not have detected the fraud.

3. Targeting specific precincts to depress turnout favorable to one candidate (a denial of service attack). This would have been a very easy attack, since the machines were left in a publicly accessible location the night before the election. All the attacker had to do was to remove the second level of tamper evident tape, since poll workers had been instructed to request new voting machines if the tamper evident tapes had been removed. Since we were barely ready by opening time, bringing in new machines would have delayed the opening of the polling station by at least an hour or two. If there were a widespread attack that removed the tamper evident tape from machines in many voting places, it is highly likely that the county would have been incapable of replacing all of the suspect machines.

Fortunately, there is a possible fix if tampering has been detected or there is a denial of service attack, namely emergency paper ballots. Every polling place should have a large supply of emergency paper ballots that can be used in emergency situations. Furthermore, a manual count should be made of the emergency paper ballots in all suspect polling places **in addition to** any manual counts that are done to satisfy a random manual audit.

Voters with disabilities.

While HAVA was passed in response to problems with the 2000 elections, much emphasis has been given to the HAVA requirement that voting be made accessible for people with disabilities. However, security and accessibility are not mutually exclusive goals. We can and should have secure accessible elections.

I cannot stress enough that I strongly agree that people with disabilities should be able to vote privately and independently and that they should be able to verify their votes. I do not know a single computer security expert who opposes non-visual access for blind voters or access to the ballot by any person with a disability.

It bears repeating that HAVA does not mandate the exclusive use of electronic voting machines to meet accessibility requirements. HAVA states accessibility can be met "...through the use of at least one direct recording electronic voting system *or other voting system equipped for individuals with disabilities*..." [emphasis added].[3]

There is a growing body of evidence that people with disabilities - blind and visually impaired voters, voters who have limited mobility and dexterity, and people with other disabilities - are finding that DREs or touchscreens are not meeting their accessibility needs and are in fact preventing them from securing a private and independent ballot.

Aleda J. Devies, a retired systems engineer, and member of Handicapped Voters of Volusia County, made the following statements in her August 01, 2006 article, *Touch Screens Are Not The Best Choice For Disabled Voters*:[4]

A key point has been lost in the various arguments for and against touch-screen voting machines. The spirit and intent of the accessible voting law are to allow every disabled person the opportunity to cast his or her [sic] privately and independently. The key word in the preceding sentence is "every." It is not acceptable to accommodate some members of the disabled population and expect the rest of us to live with "business as usual." That is discrimination, which is not legal.

Accommodating people with different disabilities requires great flexibility in a voting system. What works for and is preferred by certain members of the blind and visually impaired community does not accommodate people with mobility or motor impairments. That is one specific shortcoming with touch screen machines. People with limited use of their hands and arms may not be able to use the touch screen machines. People with spinal cord injuries or similar disorders may require binary devices such as such as "sip-and-puff". (Other binary devices include foot pedals, joy-sticks and gel pads.)

Devies also observes that, "Touch screen machines with telephone-like keypads do not meet Section 508 of the Rehabilitation Act of 1973 requirement that keypads must be operable with one hand and shall not require tight grasping, pinching, or twisting of the wrist."

Kelly Pierce, a nationally-known advocate for people who are blind and visually impaired, reviewed four voting machines in his March 15, 2005 report for the Cook County State's Attorney's Office, *Accessibility Analysis of Four Proposed Voting Machines*.[5]

Pierce analyzed tactilely discernable controls, spoken prompts, visual display, poll worker assistance, volume control and normalization, and ballot review. He found all four machines deficient in one or another of these areas.

Pierce stated, "Unfortunately, if any one of the four machines were to be deployed in Chicago or suburban Cook County as exhibited on March 15, many voters with disabilities, particularly blind voters, would not be able to cast a ballot independently and privately".

In his conclusion, Pierce remarks, "This review and those conducted by the American Foundation for the Blind, Manhattan Borough President C. Virginia Fields with The Center for Independence of the Disabled in New York, and a blind computer scientist and electrical engineer all have found that while the electronic machines represent a significant advance in accessibility from the current poll worker assistance system they often fail to effectively communicate the voting process to audio voters or are physically designed in a way that does not meet the current consensus on accessible design as

crafted by the technology industry, the disability community, and leading national governmental institutions."

Pierce's observations appear to have been born out by the voting experience of Noel Runyan, a blind computer scientist. Runyan, who has worked in human factors for well over thirty-five years, started his own company to supply access technologies for the visually impaired. Quoting just a small portion of Runyan's essay in frustration from his 65 minute voting experience in the 2004 Presidential election:[6]

It took me 30 minutes to work my way through the ballots and make my selections. After that, I had quite a bit of trouble getting into the review mode, to get a full list of all my selections. When I did, it went on and on, for 23 minutes, like a long uncontrolled drink from a fire hose. The review function read each item, and then, at the very end, said what my selection was for that item. It even threw in the details of what the fiscal impact would be, and took forever. This is completely backwards. It should announce the name of the item, then state my selection, and then read the rest of the information for that item. Also, I should have the control to press the arrow key to move forward or backward through the items, without having to listen to all the text about an item.

When I did find that I had made a mistake in my selections, I had to wait until the end of the whole review process to correct it, instead of being able to stop, make the change, and then continue with the review where I left off.

I did not want to abort the ballot verification review, to make a correction, and then have to start the 23 minute review all over again. When I later attempted to change one of my selections from "no" to "yes", the machine would not let me just select "yes", until I had first gone to the "no" entry and deselected it. This was very awkward and confusing. My wife said that she also had the problem when she was voting visually on her DRE machine.

Blind and disabled voters want and deserve secure voting systems. Natalie Wormeli, a lawyer who is completely blind, has manual dexterity issues, and uses a wheelchair[7], is far more eloquent than I could ever hope to be in her in her 2004 testimony before the California State Senate Elections and Reapportionment Committee, :

I deeply regret that I am unable to testify in person at today's hearing because of serious health problems. Please consider the following as my written testimony. I am writing this letter as a concerned California voter, an attorney, and a woman with multiple disabilities. For purposes of this letter, I am only representing myself, and I do not claim to speak for anyone else.

...

I am particularly offended by the reoccurring claim that people with disabilities are disenfranchised. This is highly inflammatory rhetoric, ignoring the definition of enfranchisement, which is a person's right to vote. When I turned 18, I became enfranchised. Not having the ability to vote without another human being's assistance is the reality that I deal with, but does not make me disenfranchised. I rely on other people

to help me with tasks that I am not physically able to do, but I remain in control and independently thinking the entire time. When voting, I can choose to bring a friend, a family member, or ask one of the well-trained poll workers for assistance.

...

Providing flawed DRE systems would erode trust among voters with disabilities as well as able-bodied voters in California and throughout the country. If Californians depend on flawed systems, and California has problems in November, the headlines throughout the country will undoubtedly reflect this horrible fact.

Other disability rights advocates claim that decertification would be a step back, treating people with disabilities as second class citizens. I argue that requiring California voters to use dangerously flawed DREs will be forcing second rate technology on us all.

I know that DRE system developers are working tirelessly to create dependable secure systems, and I am confident that one day I will be able to vote privately without assistance. However, I refuse to act as a complaining passenger in the backseat asking, are we there yet? I know I will be there soon enough, but I only want to arrive safely and with everyone on board. I know that when SB 1723[8] is passed, you will be heroes for all the citizens of California, especially voters with disabilities.[9]

For many people with disabilities, using a VVPB presents no accessibility difficulties whatsoever and does not in any way prohibit private and independent voting. Fortunately, we do not have to settle for voter verified paper ballots that are not accessible to blind and visually impaired voters. It is not difficult to integrate audio capabilities into the design stage of voting systems. Tactile ballots and tactile voting systems allow blind voters to vote privately and independently and to verify their votes. New technologies can and should be developed. For example, hand held text-to-speech reading devices, such as the one recently announced by the National Federation of the Blind, might be modified for use in elections.[10]

It's time for us to demand of our voting systems that, in addition to being accessible, they must be safe, accurate, reliable, secure, and audited. For now that means that we need voter verified paper ballots, routine random manual audits, improved policies and procedures, increased transparency, and a national mandate that voter verified paper ballots shall be the official ballots used and the final authority in all cases of recounts, challenges, random manual audits, equipment malfunction, and suspect polling places. As President Reagan said: Trust, but verify.

It is part of our nature to rely on technology to improve our institutions. Voting and voter registration are no different. Technology, if engineered and tested carefully and if deployed with safeguards against failure, can reduce error rates, provide more accessibility, increase accountability, and strengthen our voting system. However, we have rushed to put technologies in place without careful regard as to how they must perform. We are now seeing questions raised about the security, reliability, accessibility, and usability of these machines. We can take immediate steps to address security concerns by ensuring that we have voter verified paper ballots and routine random

manual audits. Beyond this, the technical community and the election community need to work together to develop computerized voting and electronic registration systems that truly deserve the public's trust.

Appendix: Electronic Voter Registration Databases

While beyond the scope of this hearing, we are seeing serious problems with statewide electronic voter registration databases. One of HAVA's key provisions requires all states to have statewide electronic databases in place by the beginning of this year. Some states already had these systems in place; others were faced with difficult decisions on how to consolidate or synchronize disparate local databases into a statewide system. Like all technology, these systems are complex and require careful engineering so that they are accurate, private, secure, usable, and reliable. Otherwise, voters can be rejected at the polls and disenfranchised, or the systems could be exposed to fraud from unauthorized access. USACM released a study earlier this year[11] that provides 99 recommendations for state and local officials to follow when implementing electronic voter registration databases.

---

[1] http://www.acm.org/usacm/Issues/EVoting.htm

[2] http://www.lwv.org/AM/Template.cfm?Section=Reports_from_Convention&Template=/MembersOnly.cfm&ContentID=5597

[3] http://www.fec.gov/hava/law_ext.txt

[4] http://www.votetrustusa.org/index.php?option=com_content&task=view&id=1595&Itemid=26

[5] http://www.votersunite.org/info/KellyPierceReport3-05.htm

[6] *Voting experience in November 2004 Election in Santa Clara County California – Using Sequoia Voting Machines*, by Noel Runyan, http://www.votersunite.org/info/RunyanOnSequoia.htm

[7] Wormeli's description of herself given in testimony at the Meeting of the State of California Secretary of State Voting Systems and Procedures Panel, April 28, 2004, Sacramento, CA., http://www.ss.ca.gov/elections/vsptranscript0428.pdf

[8] SB 1723, which would have required that all voting machines produce an Accessible Voter Verified Paper Audit Trail (AVVPAT) by some deadline. Later in 2004 SB 1438, which essentially prohibited the deployment of voting machines that did not produce an AVVPAT by 2006, became law.

[9] Testimony before the California State Senate Elections and Reapportionment Committee, by Natalie Wormeli, Esq., May 5, 2004. Wormeli's complete written testimony can be found at http://www.wheresthepaper.org/NatalieWormeli.htm or http://www.leagueissues.org/cdrom/disabled/Security.doc .

[10] *The Kurzweil-National Federation of the Blind Reader: The Revolution* Is Here!, by James Gashel, http://www.nfb.org/Images/nfb/Publications/bm/bm06/bm0607/bm060703.htm

[11] *Statewide Databases of Registered Voters: Study of Accuracy, Privacy, Usability, Security, and Reliability Issues,* February, 2006, www.acm.org/usacm/vrd.

The CHAIRMAN. Next we turn to Mr. Keith Cunningham who is the election director in Allen County, Ohio. He serves on the board of advisors to the Election Assistance Commission and also participated in the Cuyahoga County recount study performed by the Election Science Institute.

Mr. Cunningham, you are recognized.

STATEMENT OF KEITH CUNNINGHAM, ELECTION DIRECTOR, ALLEN COUNTY, OH

Mr. CUNNINGHAM. Thank you, Mr. Chairman, and let me say what an honor it is for a guy from a small town in Ohio to be sitting here before you today in this tremendous forum.

I am also the immediate past president of the Ohio Association of Election Officials, and I want to say to you before I begin, when I wake up in the morning and head for my job I am feeling pretty good about it. I believe the job that I am involved in, which is an elections director, has meaning and has merit and is doing things to make our country and our community better.

One thing I think we all agree on is that electronic voting needs some type of verification system, some component that allows it to be audited. And of course all systems need that, but as my predecessors have said, a hard ballot system is rather obvious how we audit those. Personally I do not have any particular aversion to voter-verified paper audit trails.

However, in Ohio the system is that the voter-verified paper audit trail becomes the official ballot of record for recount purposes. I must say to you, clearly I am adamantly opposed, based on the experience I have had in Cuyahoga County, to that. I believe that program is setting election officials up for failure at this point in time.

If the VVPAT was to be extended to voters as a courtesy by which to check their votes, I have no problems with that. I think statistics indicate voters don't even use it when it is available to them. The studies on hand show that maybe less than 10 percent of the people actually utilize that.

We looked at approximately 350 VVPAT tapes in Cuyahoga County, and over and over and over we encountered tapes that were missing, that were in some way compromised. You have the numbers before you, so I won't bore you with the statistics, but I think two of them are very important for you to remember. Nearly 17 percent of the VVPAT tapes reviewed by that team—and that team consisted of a lot of Ohio election officials that came in to help participate—nearly 17 percent of those tapes showed a vote discrepancy of one to five votes from the electronic machine, and nearly 10 percent of those tapes were either destroyed, blank, missing, taped together, or in some other way compromised.

My point is this: that when you use the VVPAT at this point in time as the official record of a recount vote, it actually serves to disenfranchise the voter because votes are lost in the VVPAT process. They are simply not there and cannot be retrieved. We could have retrieved those votes by other means from those machines, but in Ohio we are not allowed to because the recount official ballot of record in a recount becomes the VVPAT.

So I would submit to you that it was the paper that actually caused the count to be in question. Additionally, and we have some photographs here I would like to show you, there is no reliable technology for which to recount VVPATs. To ESI's credit they had a makeshift kind of crank thing that you could put the tapes in and reel them up. These things are sort of like wrestling octopuses.

As you can see—let's go to the next one, the next one. These are some of my friends.

This is just kind of the scene. There you can see the machine. I will tell you what I equate this to. We are pretty agricultural in my part of Ohio. I equate this to planting several hundred acres of wheat with a million-dollar planting machine and harvesting it by hand like the Amish used to, and stacking it up in the fields.

This was mind-numbing, to say the least. Now keep in mind we went through 300-some tapes. There were probably near 4,000 tapes in Cuyahoga County. This took us two 10-hour days, actually 2½ because the first half day was upsetting the system.

Continue, please.

This is simply a tape with no record printed on it. Continue again, please.

Same thing. This is the information that we are looking through on the tapes trying to—and, remember, at least this is Ohio's rule, that when you recount a race, you can't recount any other race. You can only recount the race that is going to be recounted. So if you have got 27 candidates on the ballot, you have got to reel through all 27 to get to the race, maybe a down ballot race.

This is an example of one that is taped together that has obviously been in the machine, it accordioned in the machine. I don't know, that black line probably represents 20 or 30 votes. There was no way to reconcile that. There is another torn tape, another shot of the crude machine we were using to do this.

I think they speak for themselves. I honestly don't have any reason to believe DREs don't record votes accurately but I understand the concerns and I do believe that we should have some kind of audit system for it. I would say to you, considering the size and scope of the deployment of voting machines in the last 12 to 24 months in America, I think election officials have done a pretty darn good job. We are working on improving it.

Unfortunately, I believe—and I will wrap up here in just a second—I believe it is the environment which is slowing our pace of improvement. As a local election official I am going to tell you, I feel like I am in a cross-fire, and I know many of my colleagues do; and that cross-fire is a very, very polluted conversation, and it is being polluted with political interests, corporate interests and scientific one-upmanship. And I often wish I had as many people helping me find the solutions as I did identifying the problems. It would make my job an awful lot easier.

I want to echo the remarks earlier, that I do believe we should continue to fund HAVA. I think the underfunding of HAVA sends a very inconsistent message to those of us out there trying to do this on a daily basis. I would say to you also, please allow us to finish what has been started and what is in motion before we begin to tinker with this. We have been given a set of tasks that are very, very hard to manage. And, again, in the scope of the deploy-

ment that has taken place in this country, I don't want to say there weren't problems in it, but I think my colleagues have done a very good job and I would hope that in the future when we do begin to debate and speak about this, we can do it in on honest and direct terms, without misrepresentations, half truths, and focus on what it is we need to do to cure these problems and make America's elections—give people confidence in them. I think it is too far to—too much to expect any less than that.

Thank you for your time. I appreciate it.

The CHAIRMAN. Thank you.

[The statement of Mr. Cunningham follows:]



VOTER VERIFIED PAPER AUDIT TRAILS

Testimony of

Keith A. Cunningham
Director
Allen County Board of Elections
Lima, Ohio

U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON HOUSE ADMINISTRATION
Vernon J. Ehlers, Chairman

September 28, 2006

WASHINGTON, DC

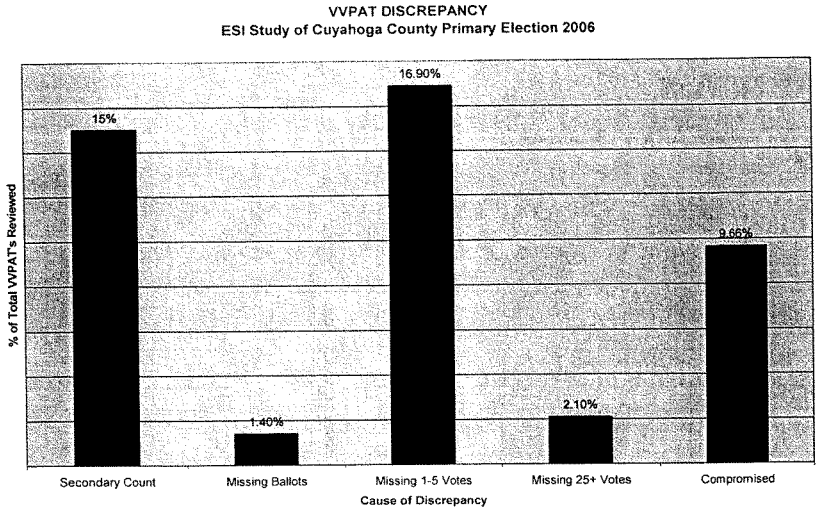
Chairman Ehlers and members of the Committee on House Administration it is an honor to come before you. Thank you for allowing me to share my thoughts. My name is Keith Cunningham, and I currently serve as Director of the Allen County Board of Elections in Ohio. In addition to my current duties, I am the immediate past president of the Ohio Association of Election Officials and a member of the EAC Advisory Board.

One thing I think we all agree on is Electronic Voting Machines or DRE's must possess some sort of meaningful and accurate audit component if they are to be seriously considered part of our voting future. Of course all balloting systems must have components which allow for vote verification. However, the means by which we can verify hard ballot systems such as optical scan are obvious so I will confine my comments today strictly to DRE's.

Personally I do not have any particular aversion to Voter Verified Paper Audit Trails. However, I am adamantly opposed to any program such as Ohio's, which makes a VVPAT the **official ballot of record for recount purposes**. To consider the VVPAT a courtesy extended to the voter as a means by which to check their vote is a reasonable proposition, even though current data does not indicate voters utilize such tools when available.

The thought that VVAPT's are reliable enough to be used as an official ballot for recount purposes is simply wrong in my opinion. I witnessed this first hand when I participated in the ESI audit of approximately 350 VVPAT tapes from the 2006 Primary Election in Cuyahoga County Ohio. Time and time again during this exercise the counting teams encountered VVPATS, the voted paper ballot produced by DRE's, which were either missing entirely or missing votes because of printer errors. The ESI study concluded:

15% of the VVPAT's reviewed required a secondary count.
1.4% of the VVPAT cartridges exhibited missing ballots.
16.9% of VVPAT tapes showed a discrepancy of 1-5 votes.
2.1% showed a discrepancy of over 25 votes.
9.66% of the tapes were either destroyed, blank, missing, taped together or otherwise compromised.



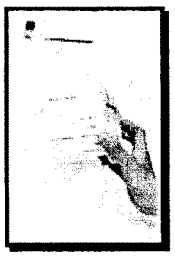
My point in all of this is that the PAPER requirement on the DRE caused discrepancies in vote totals;

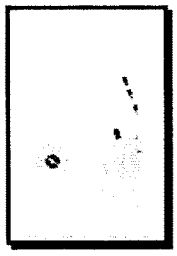
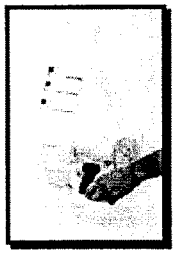
- Because the paper record was the "official" vote it now disenfranchised voters because their votes are lost to the process even though we could faithfully retrieve them from the electronic record.
- The paper caused the count to be in question because there weren't enough of the paper records to match the actual voter's votes due simply to the fact these paper systems are not ready for real time use.
- Failures of equipment caused by the paper requirements complicated the process for poll workers and VOTERS alike.

Additionally, there is no technologically reliable means by which to count VVPAT's. Several manufacturers indicate they have them in production but I have never witnessed one in successful operation and I don't know anyone who has. Thus, the methods currently employed to recount VVPAT's are makeshift at best.

AUDIT of VVPAT

Election Science Institute Audit of VVPAT
Cuyahoga County Ohio 2006 Primary Election




One of the obvious reasons for this is VVPAT was an afterthought in electronic voting. Most State VVPAT regulations were promulgated after local boards had made the decision to purchase DRE's. In some cases xpensive computerized voting systems have simply been retrofitted with cheap printers with nothing more than a **hope** their results can be matched. The fact is, the printer technology currently being utilized for VVPAT printing is woefully inadequate. Without significant and probably expensive improvement in this technology the goal of matching a VVPAT to its' electronic counterpart most likely will **not** be achieved.

I have no reason to believe that DRE's do not record votes accurately other than theories that some sort of manipulation could occur and I have absolutely no knowledge of that actually happening. That is not to say we should rely on them absent of some sort of auditing standards. However, I am convinced the VVPAT is **not** that standard.

In considering the overall issue of machine security we must remember that the parallel goals of access and ecurity are actually opposite goals in most traditional applications. Usually when we want to secure something we limit access. In contrast when something is accessible, the accepted norm is that security is going to be somewhat sacrificed. Considering the antithetical nature of these two goals I believe the election administrators across America are doing **"a pretty darn good job."** Can it be improved? Yes. Is it being improved? **Absolutely!**

I believe it is the environment, which is slowing the pace of improvement. Today, Election Officials find themselves in crossfire. That crossfire is a polluted conversation about what is really happening. The conversation is being polluted by political interests, corporate interests and scientific one-up-man-ship. It is a dialogue where fiction becomes fact and myth becomes legend. In Ohio for instance, no one even bothered to consider that the exit polls could be wrong!

"Discrepancies between early exit poll results and popular vote tallies in several states may be due to a variety of factors and do not constitute *prima facie* evidence for fraud in the current election"

INTERM REPORT ON ALLEDGED IRREGULARITIES IN THE UNITED STATES PRESIDENTIAL ELECTION OF 2 NOVEMBER 2004
THE NATIONAL RESEARCH COMMISSION ON ELECTIONS AND VOTING
A PROJECT OF THE SOCIAL SCIENCE INSTITUTE
22 December 2006

Ladies and Gentlemen, we need your help. HAVA needs to be completely funded immediately so what has been initiated can be completed. Universal, realistic standards must come forth sooner than later so that we are all speaking the same language. And when we speak, we must pledge to purge our conversation of misrepresentations and half-truths and focus ourselves on honest debate about the future of our elections in America. It is far too important to expect less.

Again, thank you for the opportunity to share these thoughts with you.

204 N. Main Street
Lima, Ohio
Phone (419) 223-8530

Keith A. Cunningham C. E. R .A.

Professional experience

Allen County Ohio
Director, Board of Elections 1998-present

Additional professional experiences

City of Lima, Ohio
Member, Lima City Council 1987-1991
President, Lima City Council 1992-1998

Martin Printing Company, Lima, Ohio
Owner, Managing Partner

Professional memberships

Ohio Association of Election Officials
President – 2005

Member, Board of Trustees

The Election Center
C.E.R.A. Program Graduate

Professional appointments

Ohio Secretary of State
Election Systems Study Committee (2000)
Voter File Update Committee (2001)

Ohio Association of Election Officials
Education Committee (2003-2004)
Board of Trustees
President – 2005

The Election Center
National Election Reform Task Force

United States Election Assistance Commission
Advisory Board

The CHAIRMAN. We hear your cry for help; namely, leave us alone, let us do it. I also want you to know that you are not the only one who has crowds of people yelling at him for a solution and offering no assistance. We experience that every day of the week. So you have our sympathy.

Next, I am pleased to introduce, James Dickson, Vice President of Government Affairs for the American Association of People with Disabilities. He has been a very strong advocate throughout this process of making certain that anyone with disabilities is permitted to vote and has the sanctity of the secret ballot which is essential to all of us and essential to democracy.

Mr. Dickson, you are recognized.

STATEMENT OF JAMES DICKSON, VICE PRESIDENT OF GOVERNMENT AFFAIRS, AMERICAN ASSOCIATION OF PEOPLE WITH DISABILITIES

Mr. DICKSON. Thank you, Chairman Ehlers, members of the committee. I have two disabilities: I am blind and I am blunt. In these 5 minutes I am going to summarize some of the points of my written testimony. First I want to thank the Members of Congress who passed the Help America Vote Act. I voted secretly and independently for the first time 2 years ago; for the second time just a month ago. I cannot put into words the glorious feeling and the pride that I had as an American, and I am speaking for tens of millions of other Americans who have now the first opportunity to vote privately and independently.

I have got a few stories to tell about the problems that I faced and which millions of other voters face when not being able to vote privately or independently. These happened to me, but literally there are millions of stories like it. The very first time I voted, the poll worker said to me, loud enough for everybody in the polling place to hear: You want to vote for who?

On another occasion I had a poll worker say to me: We are very busy; nobody votes for state legislators and these other races, so how about if we finish now?

On another occasion I had a poll worker say to me: These referenda today are really confusing, most people don't vote on them, so why don't we stop now?

On yet another occasion I had a poll worker say to me: This print on the referenda is too small, I can't read it to you, so can we be finished? That particular excuse did not get much sympathy from me.

Touch screens are the best existing product we have that offers accessibility to the greatest number of people. I participated in the earlier work that was referenced, by Kelly Pierce. The rest of the story is that after those initial tests, the company was able to inexpensively and quickly make changes to the access procedures so that the problems were eliminated.

Touch screens—access is a continuum and we need to have equipment designed so that as access increases it can be cheaply, efficiently, and quickly installed on the equipment. Touch screens are the only product available now that meets those requirements. At AAPD we absolutely want secure, accurate, recountable elec-

tions that are systems that are accessible. The paper trail is not accessible.

This is a California ballot. Try recounting. I will leave for the committee—this is the roll that was not able to be counted in Ohio. Paper trail is a Rube Goldberg contraption. It doesn't work, it is not accessible, you can't recount it. It doesn't even offer verification. Not only do people not look at the verification, in the tests done at the MIT where the computers were set up so that votes were changed, MIT students didn't find the changed vote when they looked at the verification on paper. When the verification was done by audio, listening through earphones, they found the changed votes.

I want to sum up with the following three points. Things have to be accessible. Thank you for making that stand in HAVA. The paper trail does not even do what the proponents want, and the proponents are a very small group who speak very loudly. There have been, over and over again, public opinion polls. When voters use touch screens they trust them 80 percent; 80 percent when they use them. We shouldn't let a loud vocal minority using fear determine what is going to happen in the sanctity of the polling place.

The last point I want to make, and it is very, very important, is the real problems in our voting system are human factors, are human errors. And before we order something to be done in the polling place, we need money to research and document what the problems are and we need to test proposed solutions in the reality of the polling place, not in a laboratory. Put me in an empty room with a ballot box full of paper, and I will hack into it in less than 60 seconds.

Thank you again. This discussion is very important. And I would just ask you to remember that 80 percent of Americans who vote on touch screens believe their vote is secure and accurate.

The CHAIRMAN. Thank you, Mr. Dickson. Appreciate your comments.

Thank you, Mr. Dickson, and we appreciate your comments about showing why it was so worthwhile for us to insist that all individuals be able to cast their ballot in secret. So thank you.

Next I am pleased to introduce Michael Shamos. He is a professor at Carnegie Mellon University and is also the director of the Institute for Software Research. Dr. Shamos, you are recognized.

STATEMENT OF MICHAEL I. SHAMOS, PROFESSOR, INSTITUTE FOR SOFTWARE RESEARCH DIRECTOR, CARNEGIE MELLON UNIVERSITY

Mr. SHAMOS. Thank you, Mr. Chairman. I just want to make a small correction to the record. I am not the director of the Institute for Software Research, I am just a member of the Institute for Software Research. But I am also an attorney admitted to practice in Pennsylvania and before the United States Patent Trademark Office. Since 1980 I have been an examiner of electronic voting systems for various States. I am currently an examiner for Pennsylvania and I have personally performed 118 voting systems examinations. I am going to do my 119th examination next week.

I recall that, Mr. Chairman, you are a physicist, Representative Holt is a physicist. I am a former physicist. My proposal is we settle this issue like physicists, based on scientific evidence and not on emotion.

I view electronic voting as primarily an engineering problem that includes the design of processes and procedures. Once the requirements for a voting system are agreed upon, it is then a matter of developing and manufacturing the equipment processes that meet these requirements. The question is whether Congress should be setting technical performance guidelines and engineering standards, as H.R. 550 would have it do, or whether such guidelines should be left to this and the EAC, as HAVA has already provided.

The proposed bill is based on three major assumptions, all of which are false. First, it assumes that paper records are somehow more secure than electronic ones, a proposition that has been repeatedly shown to be wrong throughout history. Second, it assumes that voting machines without voter-verified paper trails are unauditable because they are claimed to be paperless, which is also false; they are neither paperless nor unauditable. Third, it assumes that paper trails actually solve the problems exhibited by DRE machines, which is likewise incorrect.

The reason that mechanical voting machines were introduced over a century ago was to stop rampant fraud involving paper ballots. H.R. 550 would restore us to the year 1890 when anyone who wanted to tamper with an election needed to do no more than to manipulate pieces of paper. The recent example in Cleveland, Ohio, Cuyahoga County, is extremely instructive. That was the case we just heard, that 10 percent of the paper trails could not be read. H.R. 550 provides that in the event of any inconsistency between electronic and paper records, the paper records are irrebuttably presumed to be correct. Attorneys like myself are always wary of irrebuttable presumptions. Applying that provision to Cleveland would have resulted in the disenfranchisement of 10 percent of the electorate because their paper records could not be read.

I cannot believe that the numerous sponsors of this legislation contemplated such an outcome. I did a review of the U.S. elections starting in the year 1824 when the popular vote began to be kept. I looked at the percentage of times that you took 10 percent of the popular vote and subtracted it from the winner and gave it to the loser, how often would the outcome change; and the answer is, since 1854, 55 percent of our Presidential elections would have been reversed if you couldn't count 10 percent of the paper trail.

The argument is made that security problems with DRE voting demand remediation of the type proposed in the bill. Indeed Professor Felten at Princeton, Harri Hursti, and others have done a great service by exposing security vulnerabilities in voting systems. Some of these vulnerabilities are severe and require immediate repair, but the point is that they are easily remedied.

The question for the committee is what the proper response to such discoveries ought to be. When tainted spinach was found in California, Congress did not ban the eating or distribution of leafy vegetables, even though at least one human life had been lost. The appropriate reaction to the discovery of a security flaw in a voting

system is to repair it, not to outlaw an entire category of voting machines with which we have a quarter-century of experience.

It is claimed that observed reliability problems with DRE machines will be alleviated by adding a paper trail. Field experience has shown the opposite. The failure rate of paper-trail DREs is double that of DREs without paper trails. It should be obvious that adding a new device with moving mechanical parts to an existing electronic machine cannot improve its reliability.

The effect of H.R. 550 would be to ban electronic voting entirely in Federal elections. I want to repeat that. It would be to ban electronic voting entirely in Federal elections. The reason is that the bill sets forth conditions that are not met by any DRE system currently on the market in the United States. If it were to pass in its present form there could be no more electronic voting in this country, and Congress would be in the position, after spending $3 billion on new voting equipment, of spending billions more paying for what it just paid for. I cannot believe that the numerous sponsors of this legislation contemplated such on outcome.

Further, the bill as written mandates a system that would violate constitutional and statutory provisions in more than half the States. The secret ballot is regarded as an essential component of American democracy. Each one of the DRE paper-trail systems that are currently on the market either enables voters to sell their votes or allows the government and the public to discover precisely how each voter in a jurisdiction has voted. I cannot believe that the numerous sponsors of this legislation contemplated that outcome either.

I am in favor of voter verification. The proposed bill, despite incorporating the phrase "voter verified" into its title, does not come close to providing real voter verification. While it shows the voter that her choices were properly understood and recorded by the machine, it offers no assurance whatsoever that her ballot was counted, that it ever will be counted, or it will even be present in the event a recount is demanded. Once the polls have closed, the voter not only has no recourse or remedy, but is powerless to even determine whether her vote is part of the final tally or object, if she believes it isn't. That is not voter verification, regardless how it may be denominated in the text of the bill.

I submit that if Congress desires to enact a comprehensive statute mandating voter verification, it ought to verify whether the proposed legislation actually accomplishes that goal. Numerous effective verification methods are known that are not based on vulnerable paper records. These have not yet been implemented in viable commercial systems. I understand that scientists at NIST will soon announce another one.

If H.R. 550 is enacted there would be no point in continuing research and development on any such system, since the statute would prohibit any system that didn't use paper records.

Professor Ronald Rivest of MIT has recently invented a voting method that allows each voter to verify, after the election is over, that her vote has actually been counted, a feature that is absent from the systems contemplated by H.R. 550. Professor Rivest's system also allows any member of the public to tabulate the results

of the election for herself, so it is not even necessary to trust the official count.

These discoveries demonstrate that voter verification is now a ripe area of scientific research and it is far too early to mandate by statute a bad nonsolution to a presumed problem.

My purpose here today is not simply to complain about the bill but to offer a constructive alternative. As part of my written testimony, I have included a complete markup for the proposed legislation that retains its essential positive feature such as voter verification but eliminates its ill-advised provisions. I urge the committee not to report the bill favorably in its present form, and I thank you for the opportunity to be here today.

The CHAIRMAN. Thank you for your testimony.

[The statement of Mr. Shamos follows:]

Testimony of Michael I. Shamos
Before the U.S. House of Representatives' Committee on House Administration
September 28, 2006

Mr. Chairman: My name is Michael Shamos. I have been a faculty member in the School of Computer Science at Carnegie Mellon University in Pittsburgh since 1975. I am also an attorney admitted to practice in Pennsylvania and before the United States Patent and Trademark Office. Since 1980 I have been an examiner of electronic voting systems for various states. I am currently an examiner for Pennsylvania and have personally performed 118 voting system examinations. I will do my 119th next week.

I view electronic voting as primarily an engineering problem that includes designing processes and procedures. Once the requirements for a voting system are agreed upon, it is then a matter of developing and manufacturing equipment and processes that meet those requirements. The question is whether Congress should be setting technical performance guidelines and engineering standards, as H.R. 550 would have it do, or whether such guidelines should be left to NIST and the EAC, as HAVA has already provided.

The proposed bill is based on three major assumptions, all of which are false. First, it assumes that paper records are more secure than electronic ones, a proposition that has repeatedly been shown to be wrong throughout history. Second, it assumes that voting machines without voter-verified paper trails are unauditable because they are claimed to be "paperless," which is also false. They are neither paperless nor unauditable. Third, it assumes that paper trails actually solve the problems exhibited by DRE machines, which is likewise incorrect.

The reason that mechanical voting machines were introduced over a century ago was to stop rampant fraud involving paper ballots. H.R. 550 would restore us to the year 1890, when anyone who wanted to tamper with an election needed to do no more than manipulate pieces of paper. The very idea that a paper record is secure at all continues to be refuted in every election. A recent example is the May 2006 primary held in Cleveland, Ohio. That state has a VVPAT requirement. When the paper records from the election were examined by an independent study group commissioned by Cuyahoga County, ten percent of the paper records were found to be illegible, defaced or entirely missing.

H.R. 550 provides that in the event of any inconsistency between electronic and paper records, the paper records are irrebuttably presumed to be correct. Applying that provision to Cleveland would have resulted in the disenfranchisement of 10 percent of the electorate because their paper records could not be read. I cannot believe that the numerous sponsors of this legislation contemplated such an outcome.

The argument is made that security problems with DRE voting demand remediation of the type proposed in the bill. Indeed, Prof. Felten at Princeton, Harri Hursti and others have done a great service by exposing security vulnerabilities in voting systems. Some of these vulnerabilities are severe, and require immediate repair. But the point is that they are easily remedied. The question for the Committee is what the proper response to such discoveries ought to be. When tainted spinach was found in California, Congress did not ban the eating or distribution of leafy vegetables, even though least one human life had already been lost. The appropriate reaction to the discovery of a security

flaw is to repair it, not to outlaw an entire category of voting machine with which we have a quarter-century of experience.

It is claimed that observed reliability problems with DRE machines would be alleviated by adding a paper trail. Field experience has shown the opposite. The failure rate of paper trail DREs is double that of DREs without paper trails. It should be obvious that adding a new device with moving mechanical parts to an existing electronic machine cannot improve its reliability.

The effect of H.R. 550 would be to ban electronic voting entirely in Federal elections. The reason is that the bill sets forth conditions that are not met by any DRE system currently on the market in the United States. If it were to pass in its present form, there could be no more electronic voting in this country and Congress would be in the position, after spending $3 billion on new voting equipment, of spending billions more to replace what it just paid for. I cannot believe that the numerous sponsors of this legislation contemplated such an outcome.

Further, the bill as written mandates a system that would violate constitutional and statutory provisions in more than half of the states. The secret ballot is regarded as an essential component of American democracy. Each one of the DRE paper trail systems that are currently on the market either enables voters to sell their votes, or allows the government and the public to discover precisely how each voter in a jurisdiction has voted. I cannot believe that the numerous sponsors of this legislation contemplated such an outcome.

I am in favor of voter verification. The proposed bill, despite incorporating the phrase "voter-verified" into its title, does not come close to providing real voter verification. While it shows the voter that her choices were properly understood and recorded by the machine, it offers no assurance whatsoever that her ballot was counted, that it will ever be counted, or that it will even be present when a recount is conducted. Once the polls have closed, the voter not only has no recourse or remedy, but is powerless to even determine whether her vote is part of the final tally or to object if she believes it isn't. That is not voter verification, regardless how it may be denominated in the text of the bill. I submit that if the Congress desires to enact a comprehensive statute mandating voter verification, which I favor, it ought to verify whether the proposed legislation actually accomplishes that goal.

Numerous effective verification methods are known that are not based on vulnerable paper records. These have not yet been implemented in viable commercial systems. I understand that scientists at NIST will soon announce another one. If H.R. 550 is enacted, there would be no point in continuing research and development on such better methods, since the statute would prohibit the use of any system not based on paper.

Prof. Ronald Rivest of MIT has recently invented a voting method that allows each voter to verify, after the election is over, that her vote has actually been counted, a feature that is absent from the systems contemplated by H.R. 550. Prof. Rivest's system also allows any member of the public to tabulate the results of the election for herself, so it is not even necessary to trust the official count. These discoveries demonstrate that voter verification is now a ripe area of scientific research, and it is far too early to mandate by statute a bad non-solution to the presumed problem.

My purpose here today is not simply to complain about the bill, but to offer a constructive alternative. As part of my written testimony I have included a complete markup of the proposed legislation that retains its essential positive features, such as

voter verification, but eliminates its ill-advised provisions. I urge the Committee not to report the bill favorably in its present form.

I thank you for the opportunity to testify here today.

Biography of Michael I. Shamos

Michael I. Shamos is Distinguished Career Professor in the Institute for Software Research of the School of Computer Science at Carnegie Mellon University, where he directs graduate programs in eBusiness. He has been associated with Carnegie Mellon since 1975. He is Editor-in-Chief of the *Journal of Privacy Technology*.

Dr. Shamos received an A.B. in Physics from Princeton University, an M.A. in Physics from Vassar College, M.S. degrees from American University in Technology of Management and Yale University in Computers Science, the M.Phil. and Ph.D. in Computer Science from Yale University and a J.D. from Duquesne University. He is a member of the bar of Pennsylvania and the United States Patent and Trademark Office.

From 1980-2000 and from 2004-present he has been statutory examiner of computerized voting systems for the Secretary of the Commonwealth of Pennsylvania. From 1987-2000 he was the Designee of the Attorney General of Texas for electronic voting certification. He has conducted more than 115 voting system examinations. In 2004 he designed and taught a course on electronic voting at Carnegie Mellon University. In 2006 he taught a course on voting system testing for the National Institute f Standards and Technology.

Dr. Shamos has been an expert witness in five recent lawsuits involving electronic voting, including *Wexler v. Lepore* in Florida, *Schade v. State Board of Elections* in Maryland and *Taylor v. Onorato* in Pennsylvania. He was the author in 1993 of "Electronic Voting — Evaluating the Threat" and in 2004 of "Paper v. Electronic Voting Records — An Assessment," both of which were presented at the ACM Conference on Computers, Freedom & Privacy. He has provided testimony on electronic voting to the Pennsylvania legislature and to three committee of the U.S. House of Representatives.

Further information is available at http://euro.ecom.cmu.edu/shamos.html.

Markup of H.R. 550 by Michael I. Shamos, Sept. 29, 2006

[Notes: Following is a summary of the chief benefits of the bill:

- It establishes a requirement for voter verification in elections for Federal office. Because states will not invest in multiple systems in the same polling locations, the practical effect is to require verification in all public elections.
- It mandates public disclosure of voting system source code.
- It bans wireless components in voting systems.
- It provides for mandatory audits of the voter-verified records.

The bill suffers from serious deficiencies however, of which these are the most important:

- It mandates paper, the least secure form of record, as the mechanism of verification.
- It provides that the paper record would be the official record of the vote, even if the paper record is illegible, missing or obviously tampered with or defaced. This provision alone would have resulted in the disenfranchisement of 10% of the voters in Cleveland, Ohio in the 2006 primary.
- It imposes a set of technical requirements not currently met by any commercially available DRE system in the United States. Therefore, its *sub rosa* effect is to ban electronic voting entirely.
- It goes too far in requiring disclosure of source code not owned or controlled by voting system vendors, such as operating system code.
- It does not protect the disabled within the original spirit of HAVA.
- It does not go sufficiently far in requiring adherence to Federal voting system guidelines, which are presently voluntary but should be made mandatory.
- It vests audit responsibility in the EAC, which is not equipped for such an activity. Recounting 2% of the popular vote of the U.S. by hand will require 5000 people for a week, which is beyond the capacity of the EAC to administer.
- It attempts in a patchwork manner to prohibit certain conflicts of interest, but does not do so comprehensively.
- It establishes a private right of action under HAVA, which the courts have determined was not the original intent of Congress, which established an administrative complaint procedure. It will result, as has already been seen, in a flurry of frivolous lawsuits by plaintiffs seeking to outlaw electronic voting.

The markup I have provided retains the benefits while eliminating the deficiencies. Explanatory notes in brackets are provided throughout. Material that has been struck through ~~thus~~ is meant to be deleted. *[Italicized material in brackets is to be added.]*

Analysis: The apparent motivation for H.R. 550 is the erroneous assumption that DRE machines without paper trails are unauditable. They are fully auditable if the audit mechanism is tested and found to be working. All DRE machines have the capability of producing an audit trail of complete ballot images. Once it is determined that the audit

mechanism has not been compromised and is not defective, voting can proceed with the assurance that the audit trail can be used in the event of any claim of irregularity.

Even if it is believed that electronic records are subject to tampering, all the evidence is that paper records do not even begin to approach the level of security of redundant, encrypted electronic records maintained on separate physical media. The bill rests on the incorrect assumption that physical ballot security can be maintained in a highly distributed election environment open to all citizens. That is not a solved problem, and there is evidence in every election cycle of lost or mutilated paper records. As recently as May 2006 in Cuyahoga County, Ohio, 10% of the paper records maintained in the election were illegible, tampered with or missing entirely.

Nevertheless, voter verification is an important goal because of its positive effect on voter confidence. The VVPAT is a first crude attempt to provide verifiability. Unfortunately, it does so at the expense of security, secrecy, usability and reliability. It is much too early in the development cycle of verifiable systems to mandate a particular solution by statute, thus extinguishing any reason to continue research and development.]

SECTION 1. SHORT TITLE.

This Act may be cited as the "Voter Confidence and Increased Accessibility Act of 2005".

SEC. 2. PROMOTING ACCURACY, INTEGRITY, AND SECURITY THROUGH VOTER-VERIFIED PERMANENT RECORD OR HARD COPY.

VOTER VERIFICATION AND AUDIT CAPACITY.—

(1) IN GENERAL.—Section 301(a)(2) of the Help America Vote Act of 2002 (42 U.S.C. 15481(a)(2)) is amended to read as follows:

"(2) VOTER-VERIFICATION AND AUDIT CAPACITY.—

"(A) IN GENERAL.—

"(i) The voting system shall produce or require the use of an individual voter verified ~~paper~~ record of the voter's vote that shall be made available for inspection and verification by the voter before the voter's vote is cast. For purposes of this clause, examples of such a record include a paper ballot prepared by the voter for the purpose of being read by an optical scanner, a paper ballot prepared by the voter to be mailed to an election official (whether from a domestic or overseas location), a paper ballot created through the use of a ballot marking device, or a paper print-out of the voter's vote produced by a touch screen or other electronic voting machine, so long as in each case the record permits the voter to verify the record in accordance with this subparagraph.

"(ii) The voting system shall provide the voter with an opportunity to correct any error made by the system in the voter-verified ~~paper~~

record before the permanent voter-verified ~~paper~~ record is preserved in accordance with subparagraph (B)(i).

"(iii) The voting system shall not preserve the voter-verifiable ~~paper~~ records in any manner that makes it possible to associate a voter with the record of the voter's vote.

~~"(iv) In the case of a voting system which is purchased to meet the disability access requirements of paragraph (3) and which will be used exclusively by individuals with disabilities, the system does not need to meet the requirements of clauses (i) through (iii), but shall meet the requirements described in paragraph (3)(B)(ii).~~

[Notes: The above edits preserve the requirement of voter verifiability but removing the word "paper" from "voter-verified paper record" allows non-paper methods of verification. Mandating paper as a requirement removes any incentive for development of alternative methods. There would be no reason for a vendor to develop a system superior to paper if paper were mandatory.

Experience with paper trails in the field has not been good. In the 2006 Primary in Cuyahoga County, Ohio, 15% of the paper records were found to be illegible, defaced or missing altogether. See "Cuyahoga Election Review Panel, Cuyahoga County, OH Final Report (July 20, 2006), available at http://www.cuyahogacounty.us/BOCC/GSC/pdf/elections/CERP_Final_Report_20060720.pdf. Furthermore, the percentage of DREs with paper trails that fail on Election Day is approximately double that of DREs without paper trails.

The requirement in (iii) that the voting system not preserve the paper records in any way that permits associating a voter with a ballot is not met by any VVPAT DRE system currently available in the United States. Sequential paper trails, such as Diebold, Sequoia, ES&S and Hart, permit reconstruction of each voter's vote from the poll list and are completely unacceptable. The cut-sheet systems, such as Avante, print identifying numbers on the ballot which the voter may record, and thus prove later which ballot is his own.]

"(B) MANUAL AUDIT CAPACITY.—

"(i) The permanent voter-verified ~~paper~~ record produced in accordance with subparagraph (A) shall be preserved—

"(I) in the case of votes cast at the polling place on the date of the election, within the polling place in the manner or method in which all other ~~paper~~ ballots are preserved within such polling place;

"(II) in the case of votes cast at the polling place prior to the date of the election or cast by mail, in a manner which is consistent with the manner employed by the jurisdiction for preserving such ballots in general; or

"(III) in the absence of either such manner or method, in a manner which is consistent with the manner employed by the jurisdiction for preserving ~~paper~~ ballots in general.
"(ii) Each ~~paper~~ record produced pursuant to subparagraph (A) shall be suitable for a manual audit equivalent to that of a paper ballot voting system.
"(iii) ~~In the event of any inconsistencies or irregularities between any electronic records and the individual permanent paper records, the individual permanent paper records shall be the true and correct record of the votes cast.~~ *[In the event of any inconsistency between the individual permanent voter-verified records and any other electronic records, upon due investigation of the cause of such inconsistency, the records for each ballot determined by such investigation to be the more reliable shall be the true and correct of the votes cast.]*
"(iv) The individual permanent ~~paper~~ records produced pursuant to subparagraph (A) shall be the true and correct record of the votes cast and shall be used as the official records for purposes of any recount or audit conducted with respect to any election for Federal office in which the voting system is used*[, unless other records are determined under the procedure of subparagraph B(iii) to be the true and correct records]*.

[Notes: it defies logic to declare that a paper record should be irrebuttably presumed to be correct even if there is convincing evidence to the contrary. In the Cuyahoga County situation, for example, liter application of the proposed language would have eliminated 10% of the vote in the county because the paper records could not be located or read. The revision provides for an investigation in the event of a discrepancy, the results of which are to be used to determine which record are reliable.

It is a universal defect of document ballot systems (those in which the official ballot is a piece of paper) that only one original of the ballot exists. Therefore, if anyone defaces, replaces or destroys that ballot, the vote is lost.]

"(C) **SPECIAL RULE FOR VOTES CAST BY ABSENT MILITARY AND OVERSEAS VOTERS**.—In the case of votes cast by absent uniformed services voters and overseas voters under the Uniformed and Overseas Citizens Absentee Voting Act, the ballots cast by such voters shall serve as the permanent ~~paper~~ record under subparagraph (A) in accordance with protocols established by the Commission in consultation with the Secretary of Defense which preserve the privacy of the voter and are consistent with the requirements of such Act.".

(2) CONFORMING AMENDMENT.—Section 301(a)(1) of such Act (42 U.S.C. 15481(a)(1)) is amended—
(A) in subparagraph (A)(i), by striking "counted" and inserting "counted, in accordance with paragraphs (2) and (3)";
(B) in subparagraph (A)(ii), by striking "counted" and inserting "counted, in accordance with paragraphs (2) and (3)"; and (C) in subparagraph (B)(ii), by striking "counted" and inserting "counted, in accordance with paragraphs (2) and (3)".
(b) ACCESSIBILITY AND VOTER VERIFICATION OF RESULTS FOR INDIVIDUALS WITH DISABILITIES.—
(1) IN GENERAL.—Section 301(a)(3)(B) of such Act (42 U.S.C. 15481(a)(3)(B)) is amended to read as follows:
"(B)(i) 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
"(ii) meet the requirements of paragraph (2)(A) by using a system that—
~~"(I) if strictly electronic, physically separates the function of vote generation from the functions of vote verification and casting,~~
"(II) allows the voter to verify and cast the permanent record on paper or on another individualized, permanent medium privately and independently, and
"(III) ensures that the entire process of voter verification and vote casting is accessible to the voter.".

[Notes: the term "vote generation" has no meaning. Votes are not generated. The term "physically separates" is ambiguous. In any event, a technical requirement such as this belongs in the EAC Voting System Guidelines. If the rejoinder is that the Guidelines are not mandatory then they can be made mandatory for Federal elections.]

(2) SPECIFIC REQUIREMENT OF STUDY, TESTING, AND DEVELOPMENT OF ~~ACCESSIBLE~~ VOTER VERIFICATION MECHANISMS.—
(A) STUDY AND REPORTING.—Subtitle C of title II of such Act (42 U.S.C. 15381 et seq.) is amended—
(i) by redesignating section 247 as section 248; and (ii) by inserting after section 246 the following new section:
"SEC. 247. STUDY AND REPORT ON ~~ACCESSIBLE~~ VOTER VERIFICATION MECHANISMS.
"The Commission shall study, test, and develop *[effective verification mechanisms and]* best practices to enhance the *[effectiveness and]* accessibility of voter-verification mechanisms for individuals with

disabilities and for voters whose primary language is not English, including best practices for the mechanisms themselves and the processes through which the mechanisms are used."

[Notes: this subsection has been generalized to provide for the development of more and better verification mechanisms, not just improvements in accessibility.]

(B) CLERICAL AMENDMENT.—The table of contents of such Act is amended—
(i) by redesignating the item relating to section 247 as relating to section 248; and
(ii) by inserting after the item relating to section 246 the following new item:
"Sec. 247. Study and report on accessible voter verification mechanisms.".
(c) ADDITIONAL VOTING SYSTEM REQUIREMENTS.—
(1) REQUIREMENTS DESCRIBED.—Section 301(a) of such Act (42 U.S.C. 15481(a)) is amended by adding at the end the following new paragraphs:
"(7) INSTRUCTION OF ELECTION OFFICIALS.—
Each State shall ensure that all election officials are instructed on the right of any individual who requires assistance to vote by reason of blindness, other disability, or inability to read or write to be given assistance by a person chosen by that individual under section 208 of the Voting Rights Act of 1965.
"(8) PROHIBITION OF USE OF UNDISCLOSED SOFTWARE IN VOTING SYSTEMS.—
No voting system shall at any time contain or use any undisclosed software*[, subject to the exception in (i) below]*. Any voting system containing or using software shall disclose the *[specifications, designs, manuals and all other documentation,]* source code, object code, and *[any]* executable representation of that software to the Commission, and the Commission shall make ~~that source code, object code, and executable representation~~ *[the disclosed materials]* available for inspection upon request to any person.
["(i) EXCEPTION FOR COMMERCIAL OFF-THE-SHELF SOFTWARE. —
A voting system may use commercial off-the-shelf software (COTS) and the disclosure in subparagraph (8) shall not be required, provided that (1) no party involved in the design, programming, manufacture or sale of the voting system had any role in designing, programming, manufacturing or selling the COTS; and (2) the COTS was duly examined and certified pursuant to subparagraph (10) below. If the COTS has been modified in any manner, including configuration,

since its manufacture, then the disclosure of subparagraph (8) shall be required as to all such modifications.]

[This is a very significant issue, and the bill goes both too far and not far enough to provide for disclosure. Voting-specific code produced by vendors should be publicly disclosed. However, it is impractical to require disclosure of COTS source code, such as that of the Windows operating system. The revision here exempts "true" COTS, that is, COTS that has not been modified or configured by the system vendor. True COTS is exempt from disclosure only if it has passed testing by a certified laboratory.

The revision also requires disclosure of documentation and related materials along with code.]

"(9) **PROHIBITION OF USE OF WIRELESS COMMUNICATIONS DEVICES IN VOTING SYSTEMS.**—No voting system shall contain, use, or be accessible by any wireless, power-line, or concealed communication device at all. *[This prohibition against wireless devices shall not apply to infrared interfaces, provided that no such interface is accessible externally to the voting system.]*

[Notes: technical requirements such as these belong in the Voting System Guidelines, not the statute. Congress is not well-positioned to keep technical requirements up to date, or even to know which ones are advisable. The anti-wireless provision is an example of a hasty and overreaching restriction. Radio frequency wireless should be banned because of the risk of interception or interference with the signals. However, there is no reason to ban short-range (e.g., 1 cm) infrared, where the infrared components cannot be accessed from outside the device.]

[The Help America Vote Act of 2002 (42 U.S.C. 15301) is amended by deleting the word "voluntary" in each occurrence of the term "voluntary voting system guidelines.]
"(10) **CERTIFICATION OF SOFTWARE AND HARDWARE.**—All software and hardware used in any electronic voting system shall be certified by laboratories accredited by the Commission as meeting *[applicable voting system guidelines adopted as provided in section 222 and as meeting]* the requirements of paragraphs (8) and (9).

[Notes: It's time to make the voting system guidelines mandatory. Otherwise there is no assurance that voters throughout the country will be voting on systems of comparable levels of quality.]

"(11) ~~**SECURITY STANDARDS**~~ ***[CONFLICT OF INTEREST PROHIBITION]*** **FOR VOTING SYSTEMS USED IN FEDERAL ELECTIONS.**—

"(A) IN GENERAL.—No voting system may be used in an election for Federal office unless the manufacturer of such system and the election officials using such system meet the applicable requirements described in subparagraph (B).

"(B) REQUIREMENTS DESCRIBED.—The requirements described in this subparagraph are as follows:

~~"(i) The manufacturer and the election officials shall document the chain of custody for the handling of software used in connection with voting systems.~~

~~"(ii) The manufacturer of the software used in the operation of the system shall provide the Commission with updated information regarding the identification of each individual who participated in the writing of the software, including specific information regarding whether the individual has ever been convicted of a crime involving election fraud.~~

"(iii) In the same manner and to the same extent described in paragraph (8), the manufacturer shall provide the codes used in any software used in connection with the voting system to the Commission and may not alter such codes once the election officials have certified the system unless such system is recertified by such election officials.

"(iv) The manufacturer shall meet standards established by the Commission to prevent the existence or appearance of any conflict of interest with respect to candidates for public office and political parties~~, including standards to ensure that the manufacturer and its officers and directors do not hold positions of authority in any political party or in any partisan political campaign~~.

[Note: There are considerable difficulties with the above section (11). It is impractical and too narrow at the same time. Its title is incorrect since it has nothing to do with security. The notion of the "manufacturer" is not well-defined, as software is often written by one company under contract to a system vendor and it is unclear who the "manufacturer" is in such a circumstance. The term "election officials" is not defined in the statute. Most circumstances under which it is used are harmless, but this one is not. It may make sense for the chief election officer of a state to promulgate regulations for the handling of software and documenting the handling, but the provision is (B)(i) is too indefinite as to who actually has the responsibility.

The concern that programmers might have convictions for election fraud is legitimate, but surely election fraud is not the only crime that ought to be considered. (Bribery of a public official springs to mind as another.) Employers, however, often do not have

accurate information concerning their employees' pasts. The only practical way to obtain such information is through background checks.

In the end, the voter-verified ballot, combined with mandatory certification guidelines and disclosure of source code, ought to protect against even a determined criminal working for a vendor. The prohibition against officers and directors of manufacturers participating in campaigns is unnecessary for the same reason. It would also prohibit such a person from running for public office, which is the right of a citizen to do.]

"(12) **PROHIBITING CONNECTION OF SYSTEM OR TRANSMISSION OF SYSTEM INFORMATION OVER THE INTERNET.**—No component of any voting device upon which votes are cast shall be*[, or have ever been,]* connected to the Internet.".

[It is not enough to forbid connecting a device to the Internet – we must be sure it has not been connected at any time in the past, since it might have become infected with malware at such a time.]

(2) **REQUIRING LABORATORIES TO MEET STANDARDS PROHIBITING CONFLICTS OF INTEREST AS CONDITION OF ACCREDITATION FOR TESTING OF VOTING SYSTEM HARDWARE AND SOFTWARE.**—
(A) **IN GENERAL.**—Section 231(b) of such Act (42 U.S.C. 15371(b)) is amended by adding at the end the following new paragraph:
"(3) **PROHIBITING CONFLICTS OF INTEREST; ENSURING AVAILABILITY OF RESULTS.**—
"(A) **IN GENERAL.**—A laboratory may not be accredited by the Commission for purposes of this section unless—
"(i) the laboratory meets the standards applicable to the manufacturers of voting systems under section 301(a)(11)(B)(iv), together with such standards as the Commission may establish to prevent the existence or appearance of any conflict of interest in the testing, certification, decertification, and recertification carried out by the laboratory under this section, including standards to ensure that the laboratory does not have a financial interest in the manufacture, sale, and distribution of voting system hardware and software, and is sufficiently independent from other persons with such an interest; and
"(ii) the laboratory, upon completion of any testing, certification, decertification, and recertification carried out under this section, discloses the results to the Commission.
"(B) **AVAILABILITY OF RESULTS.**—Upon receipt of information under subparagraph (A)(ii), the Commission shall make the information available to election officials and the public.".

(B) **DEADLINE FOR ESTABLISHMENT OF STANDARDS.**—The Election Assistance Commission shall establish the standards described in section 231(b)(3) of the Help America Vote Act of 2002 (as added by subparagraph (A)) ~~not later than January 1, 2006~~*[within one year after funds have been made available to the Commission to develop such standards].*

[Notes: the revision ensures that the Commission will not be required to perform without funding.]

(d) **AVAILABILITY OF ADDITIONAL FUNDING TO ENABLE STATES TO MEET COSTS OF REVISED REQUIREMENTS.—**

(1) **EXTENSION OF REQUIREMENTS PAYMENTS FOR MEETING REVISED REQUIREMENTS.**—Section 257(a) of the Help America Vote Act of 2002 (42 U.S.C. 15407(a)) is amended by adding at the end the following new paragraph:

"(4) For fiscal year ~~2006~~*[2008]*, $150,000,000, except that any funds provided under the authorization made by this paragraph may be used by a State only to meet the requirements of title III which are first imposed on the State pursuant to the amendments made by section 2 of the Voter Confidence and Increased Accessibility Act of 2005.".

(2) **PERMITTING USE OF FUNDS FOR REIMBURSEMENT FOR COSTS PREVIOUSLY INCURRED.—**

Section 251(c)(1) of such Act (42 U.S.C. 15401(c)(1)) is amended by striking the period at the end and inserting the following: ", or as a reimbursement for any costs incurred in meeting the requirements of title III which are imposed pursuant to the amendments made by section 2 of the Voter Confidence and Increased Accessibility Act of 2005.".

SEC. 3. ENHANCEMENT OF ENFORCEMENT OF HELP AMERICA VOTE ACT OF 2002.

Section 401 of such Act (42 U.S.C. 15511) is amended— (1) by striking "The Attorney General" and inserting "(a) **IN GENERAL.**—The Attorney General"; and (2) by adding at the end the following new subsections:

"(b) **FILING OF COMPLAINTS BY AGGRIEVED PERSONS.**—

"(1) **IN GENERAL.**—A person who is aggrieved by a violation of section 301, 302, or 303 which is occurring or which is about to occur may file a written, signed, *[sworn,]* notarized complaint with the Attorney

General describing the violation and requesting the Attorney General to take appropriate action under this section.

[Notes: Complaints must be sworn and thus made under penalty of perjury to prevent abuse of the right of complaint.]

"(2) RESPONSE BY ATTORNEY GENERAL.—The Attorney General shall respond to each complaint filed under paragraph (1), in accordance with procedures established by the Attorney General that require responses and determinations to be made within the same (or shorter) deadlines which apply to a State under the State-based administrative complaint procedures described in section 402(a)(2).
"(c) CLARIFICATION OF AVAILABILITY OF PRIVATE RIGHT OF ACTION.—Nothing in this section may be construed to ~~prohibit~~*[allow]* any person ~~from bringing~~*[to bring]* an action under section 1979 of the Revised Statutes of the United States (42 U.S.C. 1983) to enforce the uniform and nondiscriminatory election technology and administration requirements under sections 301, 302, and 303.

[Notes: It is a great mistake to provide a private right of action under HAVA, and such was never intended, hence the administrative complaint procedure. Decisions concerning voting systems are made by duly authorized officials based on examinations they conduct and the results of studies by accredited laboratories. The experience has been that people who feel that a requirement is missing from the guidelines have been filing lawsuits alleging defects in the certification process, attempting to shift to a court the task of making technical determinations that have been left to other bodies by statute. We have already seen a proliferation of litigation of this sort. If a private right of action is conferred, the number of lawsuits will explode.]

"(d) NO EFFECT ON STATE PROCEDURES.—Nothing in this section may be construed to affect the availability of the State-based administrative complaint procedures required under section 402 to any person filing a complaint under this subsection.".

SEC. 4. PERMANENT EXTENSION OF AUTHORIZATION OF ELECTION ASSISTANCE COMMISSION.

Section 210 of the Help America Vote Act of 2002 (42 U.S.C. 15330) is amended by striking "each of the fiscal years 2003 through 2005" and inserting "each fiscal year beginning with fiscal year 2003".

SEC. 5. REQUIREMENT FOR MANDATORY MANUAL AUDITS BY HAND COUNT.

(a) MANDATORY AUDITS IN RANDOM PRECINCTS.—
(1) IN GENERAL.—The ~~Election Assistance Commission~~*[chief election official of each state]* shall ~~conduct~~*[cause to be conducted]* random, unannounced, hand counts of the voter-verified records required to

be produced and preserved pursuant to section 301(a)(2) of the Help America Vote Act of 2002 (as amended by section 2) for each general election for Federal office (and, at the option of the State or jurisdiction involved, of elections for State and local office held at the same time as such an election for Federal office) in at least 2 percent of the precincts (or equivalent locations) in each State*[, which precincts collectively shall include at least 2 percent of the registered voters of such State]*.

[Notes: It is impractical to repose responsibility for state election audits in the Commission. Each one must be conducted in accordance with state law, and they must be completed at high speed immediately following an election. A 2% mandatory hand count will result in the hand-tabulation of about 2.5 million ballots in a general election. Experiments have shown that hand-counting of ballots, including all necessary steps, takes approximately 20 minutes per ballot (Sacramento County California). If only Federal offices are hand-counted, let us assume the time would go down to 5 minutes, or 12 per hour. Counting 2.5 million ballots would take more than 200,000 man-hours, or 100 man-years. To accomplish this over a period of one week would require 5000 people. While this is only 100 per state, on average, it is far more than could be mustered and managed by the EAC. Thus the revision language hands the responsibility over to the states.

The original text would have recast the EAC as an oversight and enforcement body, which it is not equipped and was not intended to be.]

(2) PROCESS FOR CONDUCTING AUDITS.—The ~~Commission shall conduct~~*[required]* ~~an~~ audit under this section of the results of an election *[shall be conducted]* in accordance with the following procedures:

~~(A) Not later than 24 hours after a State announces the final vote count in each precinct in the State, the Commission shall determine and then announce the precincts in the State in which it will conduct the audits.~~

[(A) In every Federal election, the results of any vote count obtained at a precinct or equivalent location shall be publicly posted as soon as practicable following the close of polls.]

(B) With respect to votes cast at the precinct or equivalent location on or before the date of the election (other than provisional ballots described in subparagraph (C)), ~~the Commission shall count by hand~~ the voter-verified records required to be produced and preserved under section 301(a)(2)(A) of the Help America Vote Act of 2002 (as amended by section 2) ~~and compare~~*[shall be counted by hand and*

compared with] ~~those records with the~~ *[any]* count of such votes *[publicly posted at the precinct or equivalent location on or before the date of the election]* ~~as announced by the State~~.

(C) With respect to votes cast other than at the precinct on the date of the election (other than votes cast before the date of the election described in subparagraph (B)) or votes cast by provisional ballot on the date of the election which are certified and counted by the State on or after the date of the election, including votes cast by absent uniformed services voters and overseas voters under the Uniformed and Overseas Citizens Absentee Voting Act, the ~~Commission shall count by hand the~~ applicable voter verified records required to be produced and preserved under section 301(a)(2)(A) (as amended by section 2) ~~and compare~~*[shall be counted by hand and compared with]* ~~those records with the~~ *[any]* count of such votes *[publicly posted at the precinct or equivalent location]* ~~as announced by the State~~.

[Notes: as a general matter, states do not publicly announce vote totals prior to certification of the election, which may not occur until three weeks after Election Day. The revision would require posting of totals at each polling location, which is already commonly done, and to use the publicly posted results as the basis of comparison with the voter-verified records.]

(3) SPECIAL RULE IN CASE OF DELAY IN REPORTING ABSENTEE VOTE COUNT.—In the case of a State in which, under State law, the final count of absentee and provisional votes is not announced until after the expiration of the 7-day period which begins on the date of the election, the ~~Commission shall initiate the~~ *[audit]* process described in paragraph (2) ~~for conducting the audit~~ *[shall commence]* not later than 24 hours after ~~the State announces the final vote~~ *[public posting of the]* count for the votes cast at the precinct or equivalent location on or before the date of the election, and shall initiate the recount of the absentee and provisional votes pursuant to paragraph (2)(C) not later than 24 hours after the ~~State announces the final~~ *[public posting of the]* count of such votes.

~~(4) AVAILABILITY OF INFORMATION.—Each State and jurisdiction in which an audit is conducted under this section shall provide the Commission with the information and materials requested by the Commission to enable it to carry out the audit.~~

(b) SELECTION OF PRECINCTS.—The selection of the precincts in a State in which ~~the Commission shall conduct~~ hand counts under this section *[are conducted]* shall be made ~~by the Commission~~ on *[a]* ~~an~~

~~entirely~~ random basis using a uniform distribution in which all precincts in a State have an equal chance of being selected, in accordance with such procedures as the Commission determines appropriate, except that—

(1) at least one precinct shall be selected in each county (or equivalent jurisdiction); and

(2) the ~~Commission~~ *[chief election officer]* shall publish the procedures *[to be used]* in ~~the Federal Register~~ *[an official state publication regularly used for announcement of administrative regulations]* prior to the selection of the precincts.

(c) PUBLICATION.—

(1) IN GENERAL.—As soon as practicable after the completion of an audit conducted under this section, the ~~Commission~~ *[chief election officer]* shall announce and publish the results of the audit, and shall include in the announcement a comparison of the results of the election in the precinct as determined by ~~the Commission under~~ the audit and the ~~final~~ vote count *[publicly posted]* in the precinct *[or equivalent location]* ~~as announced by the State~~, broken down by the categories of votes described in subparagraphs (B) and (C) of subsection (a)(2). *[Such results shall be provided to the Commission within 48 hours.]*

[Notes: The above changes result from shifting responsibility for audits from the Commission to the chief election officials of the states.]

(2) DELAY IN CERTIFICATION OF RESULTS BY STATE.—No State may certify the results of any election which is subject to an audit under this section prior to the completion of the audit and the announcement and publication of the results of the audit under paragraph (1), except to the extent necessary to enable the State to provide for the final determination of any controversy or contest concerning the appointment of its electors for President and Vice President prior to the deadline described in section 6 of title 3, United States Code.

(d) ADDITIONAL AUDITS IF CAUSE SHOWN.—If the Commission finds that any of the hand counts conducted under this section show cause for concern about the accuracy of the results of an election in a State or in a jurisdiction within the State, the ~~Commission may conduct~~ *[Attorney General may require]* hand counts *[to be conducted]* under this section at such additional precincts (or equivalent locations) within the State or jurisdiction as the Commission considers

appropriate to resolve any concerns and ensure the accuracy of the results.

(e) AVAILABILITY OF ENFORCEMENT UNDER HELP AMERICA VOTE ACT OF 2002.—Section 401 of the Help America Vote Act of 2002 (42 U.S.C. 15511), as amended by section 3, is amended—

(1) in subsection (a), by striking the period at the end and inserting the following: "or to respond to an action taken by a State or jurisdiction in response to an audit *[required by or performed]* ~~by the Commission~~ under the Voter Confidence and Increased Accessibility Act of 2005 of the results of an election for Federal office or by the failure of a State or jurisdiction to take an action in response to such an audit.";

(2) in subsection (b)(1), by striking "about to occur" and inserting the following: "about to occur, or by an action taken by a State or jurisdiction in response to an audit ~~conducted by the Commission under~~ *[required by or performed under]* the Voter Confidence and Increased Accessibility Act of 2005 of the results of an election for Federal office or by the failure of a State or jurisdiction to take an action in response to such an audit"; and

(3) in subsection (c), by striking the period at the end and inserting the following: "or to respond to an action taken by a State or jurisdiction in response to an audit ~~conducted by the Commission under~~ *[required by or performed under]* the Voter Confidence and Increased Accessibility Act of 2005 of the results of an election for Federal office or by the failure of a State or jurisdiction to take an action in response to such an audit.".

[The role of enforcing the audit requirements has been shifted from the Commission, which is not an enforcement body, to the Attorney General, with the Commission in the place of recommending action to the Attorney General.]

(f) AUTHORIZATION OF APPROPRIATIONS.—In addition to any other amounts authorized to be appropriated under any other law, there are authorized to be appropriated to the Election Assistance Commission such sums as may be necessary to carry out this section.

(g) EFFECTIVE DATE.—This section shall apply with respect to regularly scheduled general elections for Federal office beginning with the elections ~~held in November 2006~~ *[held on and after one year following the date on which a voting system that conforms to the requirements of this section shall become commercially available in the United States, as the Commission shall determine].*

[Notes: It makes no sense to impose a statutory requirement that is not capable of being met, for to do so would disrupt the electoral process around the country. Therefore the revision provides for a technological development period.

Because of the statutory requirement of verification, great benefit will accrue to the first vendor who produces a conforming system, since that will start a one-year clock for compliance by jurisdictions.]

SEC. 6. REPEAL OF EXEMPTION OF ELECTION ASSISTANCE COMMISSION FROM CERTAIN GOVERNMENT CONTRACTING REQUIREMENTS.

(a) IN GENERAL.—Section 205 of the Help America Vote Act of 2002 (42 U.S.C. 15325) is amended by striking subsection (e).

(b) EFFECTIVE DATE.—The amendment made by subsection (a) shall apply with respect to contracts entered into by the Election Assistance Commission on or after the date of the enactment of this Act.

SEC. 7. REQUIREMENT FOR FEDERAL CERTIFICATION OF TECHNOLOGICAL SECURITY OF VOTER REGISTRATION LISTS.

Section 303(a)(3) of the Help America Vote Act of 2002 (42 U.S.C. 15483(a)(3)) is amended by striking "measures to prevent the" and inserting "measures, as certified by the Election Assistance Commission, to prevent".

SEC. 8. EFFECTIVE DATE.

Except as provided in section 6(b), the amendments made by this Act shall take effect as if included in the enactment of the Help America Vote Act of 2002.

[Section 101 of the Help America Vote Act of 2002 (42 U.S.C. 15301) is amended by adding at the end the following new paragraph:

"(d) FEDERAL OFFICE DEFINED.— The term "Federal office" means the office of Senator or Representative in, or Delegate or Resident Commissioner to, the Congress."]

[Notes: This change is required to preserve the constitutionality of HAVA. The term "Federal office" was used in HAVA but was not defined. Under the Constitution, Congress has highly constrained power to regulate elections for President and Vice-President, being limited essentially to specifying the date on which electors shall be chosen.

The new definition makes it clear that President and Vice-President are not "Federal offices" for purposes of the statute. The practical effect of the change may be minimal, since in regularly scheduled elections, voting for senators and representatives occurs at the same time as choosing electors for President.]

The CHAIRMAN. We will now turn to questions from the committee, and I will begin and yield myself 5 minutes for that purpose. And Dr. Shamos, since we just finished with you, let me pursue one comment you made. I could pursue many, and I am sure others will pursue those, but on the one you said paper trails are no more accurate than any other method. Let me ask if you would also include paper ballots which are then read by a computer in that category.

Mr. SHAMOS. Oh, Mr. Chairman, I don't think I actually made any comment about the accuracy of voting systems. I think I said that paper systems weren't secure.

As far as accuracy, accuracy is a very poorly defined concept in voting systems and extremely difficult to measure, because we need to know in advance the voter's intent before they go into the voting booth. Then we need to see through the entire chain of custody of all the ballots at the end whether the final tally really reflects how the voters intended to vote. That is nearly unmeasurable except in small laboratory experiments. So I actually haven't made a comment about accuracy.

The CHAIRMAN. Okay. In general, your comments about paper trails, do those also apply to paper ballots that are then scanned electronically?

Mr. SHAMOS. Paper ballots that are scanned electronically are certainly subject to the same kinds of tampering. In fact it is easier in general to tamper with those because they are cut sheet paper, individual pieces of paper. There are all sorts of problems with optical scan voting but it is certainly acceptable as a method of voting. We use it in Pennsylvania. It is in widespread use around the country.

The CHAIRMAN. Let me just extend that one little bit. In terms of recounting for—in case someone demands a recount, isn't a paper ballot a good reliable method of recounting, simply because the voters themselves have marked that particular piece of paper?

Mr. SHAMOS. No. The problem is that once the voter has marked the ballot and verified that the ballot is marked the way she wants, she has no assurance that by the time the recount occurs, that same piece of paper is going to be in the hands of the recounters.

Ms. Lofgren from Silicon Valley might recall that in the 2004 election in San Francisco, 3 weeks after the election, ballot boxes were found floating in San Francisco Bay with ballots in them. And so we have not solved the problem, security of paper ballots, in a widely distributed voting system that we have in the United States, with a couple hundred thousand precincts.

The CHAIRMAN. Thank you. I didn't realize we had that problem since the LBJ election and Tammany Hall, Prendergast, et cetera. Thank you.

And quickly I am turning to Mr. Felten, I am interested in your comments. How easily could one access the voting machine and insert a virus of the type you have commented? How long does it take to actually get the virus in place? Would someone need to access the machine for an appreciable amount of time? Or is this something that a voter in a voting booth could do?

Mr. FELTEN. It takes about 1 minute of access to the machine, and I can show you roughly what would be involved. It would in-

volve opening the door on the side of the machine, which would require getting a key. As I said, those are for sale on the Internet. There may be some security tape that would need to be removed and might be missing already. Opening up this door, putting in the memory card like this into the side of the machine—the memory card would have been prepared in advance with the computer virus on it—then pressing the red power button and waiting about 30 seconds, and afterward closing everything up and putting it back.

This is something that would be unlikely to be doable by a voter in the polling place, but if the machine is not—if the machine is not guarded with a very careful chain of custody throughout its life cycle, it can be available to that. In my polling place in Princeton, the DRE machines sit unattended overnight, the night before the election, in an unlocked school lobby.

The CHAIRMAN. How long would it take someone who had access to the machine to figure out how to write the program?

Mr. FELTEN. It requires some information about how the machine works. This is not a Manhattan Project. It requires a moderate level of skill in computer programming and some limited knowledge, probably the knowledge that has in this case—that had leaked from the vendor to the Internet a few years ago, would be nearly enough. And I think an unscrupulous person would not have a problem getting the necessary information.

The CHAIRMAN. So from the time you started looking at the machine until you devised the virus, what sort of time was involved?

Mr. FELTEN. We got the machine in May. At first we spent a lot of time taking it apart to understand everything we could about how it worked. We were interested not only in whether a virus would be possible, but we really wanted to understand all of the security mechanisms and we wanted to treat it very carefully. From the time we started developing virus code until we had a working virus, perhaps a few weeks.

The CHAIRMAN. Thank you very much. My time has expired. I am pleased to recognize my Ranking Member, the gentlelady from California.

Ms. MILLENDER-MCDONALD. Thank you so much, Mr. Chairman, and thank you again for this very interesting hearing.

The one thing I want to say about my friends in the Senate, they have a bill out now, saying that every polling place should have a large supply of emergency paper ballots that can be used in emergency situations. That is just where we are. That is what we think about voting now in this country of ours. And so Senator Dodd and Senator Boxer and others have submitted this bill.

But I have said all along that there is a security issue here. There is a trust issue that we must come to bear in terms of voters.

Mr. Felten spoke about when there aren't consequences, there are compromises—or consequences bring compromises. And I wanted him to expound a little bit on that. And he also said that existing election procedures are not adequate for elections. I want you to expound on that too, sir. And tell me, if Mr. Dickson feels a paper trail is not adequate, especially for disability, then you are suggesting, Mr. Felten, that paper trails do cut down on voter fraud. So we have some imbalance here. If you could just speak to that for me on those issues.

Mr. FELTEN. Certainly. The first issue had to do with the the consequences of the compromise being worse in an electronic system. And in the example that we gave here, there is a computer virus that will spread itself from one voting machine to others, and the consequence is that if someone is able to compromise one machine, the virus can spread to many machines and potentially affect all the votes on all of those machines, as compared to fraud with an old-fashioned ballot box where access to a ballot box only allows someone to tamper with the votes that are in that ballot box, or maybe increase them by some amount. Access to one cannot involve stealing tens of thousands of votes as with an electronic system.

Ms. MILLENDER-MCDONALD. But this virus, you say, can pass from one machine or one voter to another. I think you stated that. How can that be when I am told manufacturers do not give out this so-called code, secure code they use, how can that then be done with that?

Mr. FELTEN. Well, the way that the virus—the way that this virus spreads is on these memory cards. The memory cards are programmed before an election, usually at a central location, and they are programmed with the list of races and the list of candidates and so on for that election. Then they are distributed out to the polling places and put into the voting machines. That is a possible—that is a possible mode of travel of the virus.

If the virus gets onto the memory card at that central location, it will then be installed out into the voting machine. After the election, the memory cards go in the opposite direction to carry the votes back to the county clerk or Board of Elections Office to tabulate them, and that allows the virus to go in the other direction. So a virus in one machine may hitch a ride on a memory card, after the election, back to the election headquarters and then potentially spread there onto many other cards that are then distributed, say, for the next election.

This is much like the process by which older computer viruses spread on floppy disks. If you put an infected floppy disk into your PC, your PC would catch the virus and then it would spread to any other disk that you put into your machine. So it hitches a ride, opportunistically, on top of the flow of these memory cards that happens in running an election normally.

Ms. MILLENDER-MCDONALD. How do we answer Mr. Dickson's whole notion that paper trails are not acceptable to the disabled and yet you say cut down on voter fraud?

Mr. FELTEN. Yes, I do believe it cuts down on voter fraud and I do believe that a paper trail, well designed, can be just as accessible. Mr. Dickson held up the roll of paper and pointed out he could not view that or verify it or audit it. But the DRE system that he is advocating stores his votes on this, which neither he nor anyone else can simply look at and read. The problem with these DREs and the security problem is exactly the thing that Mr. Dickson is complaining about: the inability of any voter to look at the machine and see their vote recorded. So I don't believe that there is a conflict between the use of a paper trail and accessibility.

Ms. MILLENDER-MCDONALD. There are just so many questions that I have just put all over the place here. The whole notion, Mr.

Cunningham, that you spoke of—and I see my red light is on already. That is what I am saying, it is just so much in so little time to talk.

The CHAIRMAN. We will have a second round.

Ms. MILLENDER-MCDONALD. A second to go back?

The CHAIRMAN. Second round.

Ms. MILLENDER-MCDONALD. My second round I will come back to you, Mr. Cunningham and Mr. Shamos, because I do want to talk with you. Thank you, Mr. Chairman.

The CHAIRMAN. Thank you. The Chair recognizes Mr. Brady, the gentleman from Pennsylvania, for 5 minutes.

Mr. BRADY. Thank you, Mr. Chairman. Mr. Chairman, I have a point of inquiry. Will Mr. Holt have a chance to speak? Will he have a chance to speak?

The CHAIRMAN. By unanimous consent, we will allow Mr. Holt to speak.

Mr. BRADY. Okay. I am just—I don't think voting is a science. I think it is a people person thing. I think it is—I think it is a human thing. And I think that anything we do here, no matter what it may be, can be attacked, can be hacked into, can be verified. Ballot boxes can be put in a river, could not be shown. But I think what we are trying to show is try to eliminate as best as possible all these things that can possibly go wrong. And I don't understand why a receipt—because that is what I look at a paper ballot as a receipt—why, when you vote and you get your receipt and you have that and you see what you voted for—and if you don't have that, then you could—if you don't have that, then you can allow some type of protest somewhere. If you have no receipt, you think you voted, you don't know. It is up to now whatever tabulation or whatever machine or mechanical or scientific tabulation happens. And I don't understand why it would be a problem for anybody having a receipt.

Mr. Shamos, you heard my statement and you have inspected many times the voting machines, and from what I understand, you had said that a malicious hacker could easily make the same switch, allowing votes to be changed from one vote to thousands of votes. Then if that is the case, why are these—we think these systems aren't reliable and if that is the case, what would be the problem with a verified paper trail? If I want to vote and I want to vote for you, if I look at a paper and it says I didn't vote for you, I can lodge a complaint right there. If I walk out there with nothing, I don't know who I actually voted for. I am in the hands of that machine, a hacker or anybody who could probably get in to violate the voting process. I don't understand why this should be a problem. No matter what we do, there will still be a human factor somewhere, someplace, somehow.

At least a voter has the confidence that he has or she has a piece of paper stating that, yes, I did vote; yes, this is who I voted for. And if there is a mistake, you may have a chance to rectify it right there. That is my point.

I yield back the balance of my time. Thank you, Mr. Chairman.

The CHAIRMAN. Any answers or any comments?

Mr. SHAMOS. I can say something. It is certainly true that if a malicious hacker is able to gain access to a voting machine and re-

place the software that is in there in such a way that that change is not detected, then there are severe problems. And that is what I say, when we find security vulnerabilities, we have to find ways of plugging them.

For example, the vulnerability discovered by Professor Felten's group at Princeton was known to us in Pennsylvania back in March, right before our May primary. And we were forced to make an emergency remediation in Pennsylvania to blunt the effects of that discovered vulnerability, because we wanted to be able to assure county election officials and voters that an intrusion of the kind that was demonstrated here today was not possible, or if it had happened, the effects of it would have been reversed and so we remediated that. We also instructed the vendor that the next time it comes back for a certification, it better have remediation of its own so that we don't have to impose administrative procedures to make sure that that vulnerability can't be exploited.

So I am not minimizing the possibility that people are out there trying to hack things. My point is the response to the hack is not to throw the machines in the ocean and go back to what we were doing in 1890. If it is a technological problem, we have a technological solution.

With respect to the receipt, a lot of people think of the word "receipt" as meaning something that the voter can take home with them and look at later at their leisure and show maybe at some later time to an election official and say, see, this is really how I voted.

It is not legal to give receipts of that kind because you can't give a voter anything they can use to prove how they voted, since they could then sell their vote. So the receipts we are talking about, these voter-verified paper trail systems, the voter has a chance to view the receipt on the machine and then say yea or nay; yes, that truly represents my vote or not, and then when they leave the polling place, they don't have a piece of paper to take with them, and my point—the point that I made in my earlier testimony is that it is nice enough to show the voter that their vote was properly recorded. But, again, there is no assurance that at the time the votes are actually tallied later, or a recount was done, that that piece of paper is even around or hasn't been replaced by something else, and there are people who are working on the solution to that problem and we are not there yet.

Mr. BRADY. Mr. Chairman, if I can just answer, you are way out there. You are talking about after voting, you are talking about people manipulating receipts that they may or may not get. I mean, now you are becoming human factor after human factor after human factor, somebody is hell-bent on trying to rig an election. That is not what we are talking about. We are talking about voter confidence. That is what I am talking about. I am not talking about a receipt you take home and say, I want to change my vote or I made a mistake. Because people do make mistakes. If you make a mistake on the voting machine, you make a mistake. You can't rectify it after you validate it.

But I am saying, as you are saying, look, this is who I voted for. This is what I wanted to do. Push the okay button, push the vote button, whatever, close the curtain, open the curtain. I don't think

there is anything wrong with that. That is what I am saying. I don't think there is nothing wrong with our bill.

Mr. SHAMOS. If I told you that mechanism could be used to discover how every voter in the precinct voted, that might change your mind.

Mr. BRADY. I learned that you people with this electronic scientific, you show me anything I ever did in my entire life. So that doesn't scare me.

The CHAIRMAN. That might make for an interesting episode. Ms. Simons, quickly.

Ms. SIMONS. I just wanted to comment briefly on this whole paper issue, because I think we are comparing apples and oranges. One of the basic issues is how well engineered these systems are. And somebody who was advocating for voter-verified paper trails early on, fore the machines were retrofitted—I have to say I was appalled by what the voting machine companies came out with. They are bad.

I mean, Mr. Cunningham is right. Jim Dickson is right. The continuous rolls of thermal printed paper have privacy issues, as Michael Shamos says. But they are badly engineered. It is bad technology. There is no reason why paper has to be—why they have to be designed that way. They were the cheapest way to do it. That was why it was done that way. I mean, banks deal with paper all the time. They manage to count it. And I don't think they make many counting mistakes. Other countries vote on paper, and they don't have problems. We can do it, too, but we have to do it right. If you do it wrong, it will fail.

The CHAIRMAN. And for the last quick word, Mr. Dickson.

Mr. DICKSON. Chairman Ehlers, I wanted to respond to your question about counting optical scan ballots by machines. We have a lot of experience in this country with that. When you have large numbers of ballots, hundreds of thousands, and you have got a close race, every time the optical scan ballots have been counted you get a different number. You get a different number. We do not have the technology to accurately count large pieces of paper.

The CHAIRMAN. Right. Thank you very much.

Next the Chair recognizes the gentlewoman from California, Ms. Lofgren, for 5 minutes.

Ms. LOFGREN. Thank you, Mr. Chairman. This is a very helpful hearing, and as I am listening, it seems to me that the point made by Ms. Simons needs to be emphasized: The fact that we have a dysfunctional roll doesn't mean that that is the only alternative available as an auditable trail.

You know, I spent more years on the board of supervisors in Santa Clara County than I have so far in Congress, and in California, the counties are the repository of the registrar of voters, and in California the registrar of voters is a civil service position. It is very nerdish, I guess is the best word you could say, in Silicon Valley and very apolitical, and it wasn't really until I got on the board of supervisors that I realized—I guess I never really thought about it—that, you know, some of the votes get lost.

People don't think about that, but we had the little punch cards for a long time and it would jam up the machines on election night, and some of the ones that got mangled didn't get caught. And it

didn't ever—at a time when the country was less closely divided than it is today, nobody really noticed because elections weren't that close. But of course now we have close elections all the time, and we are paying more attention to it. And so I do think that we need to make sure—you can't have a perfect system, I suspect, but we need to have a system where people do not question the integrity of it.

I remember going with a computer scientist in my district who really said this: Yes, you can make a mistake, I mean, you can take a ballot box and throw it out, but the difference with hacking a machine is it is not random, the direction in which those votes are going to be lost.

And so I am very enticed by Mr. Holt's bill. I would know that in a standards setting, there has been discussion that this would eliminate the privacy of individuals. But on page 3, line 13, of his vote, it specifies that to comply with the act that would not be permissible.

So I think, you know, part of what we do here in Congress is to set standards and laws that need to be met, just as NIST does from an engineering point of view.

I am wondering, Mr. Felten, Mr. Shamos said something to the effect that you could verify other than by paper means. I don't want to misquote you or something; it was something to that effect. How would you do that with the virus that your lab created? How would you do a verification without—would there be a way?

Mr. FELTEN. Well, I think that the idea of nonpaper verification is something that is not ready yet. It is an active area of research. Mr. Shamos referred to Professor Rivest's work, which, by the way, is an all-paper system. And that is an interesting proposal, but I would not want to trust an election to it tomorrow. I think that years from now we may be in the position to have effective and useable nonpaper-based systems, but I do not believe they are ready yet and I don't think we can afford to wait.

Ms. LOFGREN. Mr. Shamos, your testimony has been very interesting, and thank you for your advocacy and your work on assuring systems. One of the things that you suggested, that we needed to make sure that vulnerabilities are protected again—and no one would disagree against that—but one of the things I learned in my prior life in local government was that elections, they are not chaotic but they are—they are chaotic. You have got, you know, PTA mothers and you have got volunteers, and there are schools, and it is really—I love election day, but it is not really tightly controlled and cannot be, because that is not the way Americans hold elections, unless we completely fund this and have full-time paid people. And I don't think we are moving in that direction.

So how would we be able—even if we found this virus, I know from Silicon Valley, I mean there are a million ways to hack this stuff. Given the fact we have this chaotic system, we have smart hackers everywhere, how do you protect against those vulnerabilities in your judgment?

Mr. SHAMOS. Okay. So there are several ways. One is that we are never going to achieve perfection, we are never going to locate all vulnerabilities that exist in systems because we don't know how clever people may be in the future to get around the protections

that we have built in. But this is true not just in voting systems. In every kind of system that has ever been made, there are later discovered vulnerabilities.

As I said in my testimony, I am in favor of voter verification. Voter verification is a way of assuring that if a vulnerablity has been exploited that we are going to know about it.

I think you just asked about a potential nonpaper mechanism for verification. I will give you a very simple one that the TS unit over there has a touch screen that shows things to the voter. The voter is not positive, however, that the marks that she makes that are visible on the screen are actually getting recorded by the machine. So all we have to do is have a second screen, made by a different manufacturer, and we take an electrical wire and we get a copy of whatever is on the first screen to the second screen, and we attach a digital camera to that and we make a record of what the screen showed. And if the voter has any doubt it has been recorded correctly, she can press a button that says "replay" and it will show her her vote again on the screen. And that vote gets recorded on a CD or DVD and prevents it from being tampered with later. That is just a trivial example of a nonpaper verification mechanism.

The second way of doing it is through something called parallel testing, which is used in at least 10 counties in California. It is going to be used in Massachusetts in November. It is used in several other States, where you sequester a machine or machines during the election, during the actual time of the election, and you have a team of people vote on them, simulating the way they vote, except they vote according to the predefined script so we know what the total should be at the end. Then at the close of polls, we close that machine and we see if the totals match. If they don't match, then we know that there is a rat somewhere, and we do a forensic examination to find out where the rat is.

The CHAIRMAN. The gentlewoman's time has expired. I am pleased to recognize our guest, Representative Holt, for five minutes.

Mr. HOLT. I thank the Chairman and I am pleased to see that we are holding—that you are holding this hearing, and I welcome the opportunity to be with you. And I regret that the hearing is being held the day before our target adjournment for the year. But nevertheless, I think you have put together a good panel of witnesses.

Let me just make two quick comments. One is, HAVA had the unanticipated effect of motivating jurisdictions to go out and buy devices for voting that are clear, simple, accessible, easy to use and totally unverifiable. And it may be that there are various future methods of verifying that are not yet thought of or not yet developed, but right now we have a method of verifying where each voter can verify her vote at the time of voting, and that is a paper trail. And I do think it can be made accessible for voters, for all voters.

Mr. Shamos just described a rather Rube Goldberg-ish CD camera that was going to photograph another screen. Boy, paper record sounds a whole lot easier to me.

But anyway, let me first go to Mr. Felten, Professor Felten. How detectable would the virus that you devised, or that someone might devise, be before, during, and after the election?

And let me ask another question. I don't know whether you are familiar enough with the kind of chain of custody and other checklists that Mr. Smith puts his machines through. Do you think a virus could be implanted in a system that had the kinds of protections that Mr. Smith describes?

Mr. FELTEN. First the question of how detectable this would be. There is a long-established cat-and-mouse game in the PC world between virus writers and antivirus companies, and the virus writers have proven very successful at making viruses that are quite difficult to find, especially in advance. And I would expect, or I suppose fear, that we would see the same phenomenon here. We did not try to make this virus as stealthy as we could. But I think that if someone used the same methods that are used in the PC world to make viruses hide, it would be very difficult indeed to find in advance.

Preelection logic and accuracy testing as has been discussed here will not find the virus that we devised, because it simply checks whether the machine is in logic and accuracy testing mode or real election mode, and if it is in logic and accuracy testing mode, the virus simply lies low. So I think it might be quite difficult to find, and I certainly would not have confidence that if it were implanted it could be found.

The second part of your question related to the procedures that Mr. Smith described, and I think those sorts of procedures are very valuable. They do help to close the gap, to close the window of vulnerability, but we also have to recognize that procedures are not perfect and are not always followed. Like any other part of our election system, there will be gaps, there will be errors. And I still worry, despite the best of procedures, that the window of vulnerability opens enough that a determined adversary can get through it.

Mr. HOLT. Thank you Mr. Shamos.

Yes, Mr. Smith. If there will be another round of questions, I would be happy——

Mr. SMITH. I would like to respond to that, because I think it really comes to the core of what we are trying to talk about. I have listened to the situation with regards—I am the only one here, by the way, who uses Diebolt TS units, and I am the only election director I guess on the panel that does.

One of the things I have been listening to and have been concerned about is how this virus would spread. I am an engineer by background. I hold a double E degree so I have some kind of technical capability in that.

First of all, if you took one and you corrupted this memory card—can I see your card? If you took and corrupted this memory card, and it is going to go into one machine, and that one machine in my county is probably going to vote between 100 and 150 votes, that's all that's going to be counted on it, the issue comes on this card supposedly then is it is going to be corrupted; okay, we will lose 100 votes. That is not good, but it is not like we are losing

50,000 votes that I have cast in the general election, in the last one in 2004.

Now, this comes out, it goes back to the end of the process, as Mr. Felten has said, it is only going to corrupt one more machine. The machines are not interconnected. There is not a possibility of corrupting the 500 machines that I am going to put in place for the 2006 general election. That is, you know, an issue. It is a tactic; it is not going to happen.

Now, there are a lot of other things that we do. I mean, we have a lot of security in place. We follow it. I am very anal about those types of things and I have talked to Mr. Felten about it, and I think that he believes in our county we have a good thing.

The last thing is, I would like to respond to what Ms. Millender-McDonald said—and I think this is as important as anything—is that the confidence people have in our equipment is very important. I mean, I couldn't say anything more. We take—and after every election we hand out a response card, given out randomly to our people. We say, what do you think about the process? You want to have, whatever, and I have got in front of you—it is not a technical, you know, survey of the type, but there are 715 responses. You can see the names, you can see the precincts, you can see what the election was held for; in addition, you can see their comments. 99.5 percent of the people that responded to these things in my county said we did an excellent job. There was only two people, only two that requested a paper trail.

So I think we are doing a good job in Forsyth County, Georgia. I think we are doing an excellent job in the entire State of Georgia and I think that we need to be—I don't want to say "recognized" for it, but hopefully—don't impose things on us which are going to make our job much harder to do. But I also will tell you that I agree with Mr. Felten with regards to having verification, but I believe that we do not need to eliminate the paper.

Mr. HOLT. My time has expired. I hope Mr. Felten will get a chance to reply, because on my visit to his laboratory it was my understanding that the method of spreading the virus is different than Mr. Smith seems to understand.

The CHAIRMAN. Very quickly could you give a brief response?

Mr. FELTEN. Sure. Well, without getting into a long technical debate, let me just say that when this memory card goes back to the central facility and is put into a so-called accumulator machine which adds up the votes, if that accumulator machine becomes infected it can then infect a very large number of other memory cards that are subsequently put into it, and it acts as a very serious carrier of the virus.

The CHAIRMAN. Thank you.

Just an announcement to my colleagues. I have received a note that votes are expected between 12:00 and 12:15. I would like to have a second round of questions. Let me suggest that each of us tries to limit ourselves to three minutes. And I will begin, and then recognize the minority leader or the ranking member. Mr. Doolittle presumably will be settled in by then and ready with his question.

We were just talking to Mr. Smith and I was wondering, Mr. Smith, what kind of system did Georgia have before it adopted the electronic system? Why did they see the need to change to the cur-

rent system, and what were some of the problems you experienced with the previous system? Basically, is the new system better than the previous one or not?

Mr. SMITH. Okay. I think I can respond to that. Fortunately I took over as director of elections prior to the introduction of the DRE machines. We had at that point in time the punch card machines. By the way I would say the security level we had on the punch cards is pretty miserable, now that I have gone through and listened to all the technical dissertations that have gone on. Our punch card machines were monitored by a computer as well. That computer sat in a—it was an IBM 386 or something like that. It sat in a closet that we kept, and in fact they downloaded software to it routinely, you know, over the telephone lines. I would say that was highly unsecure, and I was mortified at that when I saw it.

The changes, the changes that we had, 6 months prior to the 2002 election, Diebolt machines were introduced into Georgia. We had 6 months in which to take this across the entire State, and I would say that the secretary of state and the Center for Election Systems from Kennesaw State University did an outstanding job.

I tell you, I personally used to run major computer projects. I didn't think they could do it. They have done an outstanding job. We have continued to hold elections, and people are very pleased with them in our State.

Are there problems? I think some of the things Ms. Millender-McDonald brought up with regards to training poll workers are very valid, and I appreciate the fact that she will continue to fund it. I would like to ask if she would fund the program also so it is part and parcel of a program that I have introduced, which is called Forsyth First Vote, but we also use high school students to do it. One-third of all my poll workers are students. We have changed the entire complexion of the people in our county. Maybe that is why we are running good elections, I don't know, but I have got poll workers that we turn away because we have a very good program, and I am very pleased with it. Thank you.

The CHAIRMAN. Thank you very much.

Briefly, Mr. Cunningham, you mentioned that you grew up in a small town in Ohio. I spent my high school years in an even smaller town, I am sure, known as Celeryville, Ohio; population, 200.

I have a question for you about the VVPAT technology, the printing paper trail technology. It is relatively new. You have described the problems that you have encountered with that in Ohio. Do you believe improvements can be made to the VVPAT printer technology to make it more reliable, to capture true vote totals, to avoid the problems you have had; and then would the added complexity brought to the system always increase the likelihood of failure? Or do you think through sufficient research and study, we could make them more reliable?

Mr. CUNNINGHAM. Thank you, Mr. Chairman. I have a personal motto: I never buy the first model of anything. I always let other people figure out what the problems are before I buy. I think the fact of the matter is, when the Help America Vote Act was passed, most of the touch-screen voting machines were, by and large, prototypes and rushed into manufacture. I am not taking any issue with any of the manufacturers, and I am not making a comment on the

reliability of any of their machines. But I think what we have got on our hands here is the Model-T Ford. We are in the early stages. Now, can it be improved? Absolutely. I think throughout my comments I was very definite to say these machines as they currently sit are not reliable.

My question back to you, though, in that regard is, who is going to pay to fix it? Because one of the problems we have right now is in the last 24 months, every election jurisdiction in this country has spent the $3 billion we spoke about earlier on new election equipment, and that is what is in place. So without somebody stepping forward to fund that enterprise, I don't know how we are going to improve them ourselves.

And if I could, Ms. Lofgren, I liken running an election to throwing a package of BBs on your kitchen table, and while somebody is on each leg moving the table, you are trying to keep them all on the table all day long. That is my analogy of election day.

The CHAIRMAN. Thank you for that discouraging analogy. Next I recognize the Ranking Member for five minutes.

Ms. MILLENDER-MCDONALD. Thank you, Mr. Chairman. And let me again thank you so much for this hearing. This has been just absolutely the most informative hearing, one of the great ones we have had.

Mr. Cunningham, I thank you for saying that we all agree that some type of verification system is needed, and at least we have a consensus here for that. But you did speak of the fact that you are adamantly opposed to any program such as yours in your State which makes VVPAT the official ballot of record for recount? If I am not mistaken, Ohio lost 10,000 ballots. And what happen here, given that you were not able to recount because you can't reprint?

Mr. CUNNINGHAM. In Ohio—what election are you talking about?

Ms. MILLENDER-MCDONALD. It was my understanding that there were 10,000 votes that were unable to be recounted because you were unable to reprint.

Mr. CUNNINGHAM. You mean at the ESI?

Ms. MILLENDER-MCDONALD. Yes.

Mr. CUNNINGHAM. Ten percent of the VVPATs counted, I forget what the numbers were exactly. I believe the statement that I made was that nearly 10 percent of the tapes were either destroyed, blank, missing, taped together or otherwise compromised in some way. I don't—I don't think that it would be correct mathematically to say it was 10 percent of the votes; but 10 percent of the VVPAT tapes, based on what we reviewed, had some kind of compromise that made it very difficult to ascertain what the real numbers were.

Ms. MILLENDER-MCDONALD. But you make a valid point that because of the VVPAT, one is unable to reprint; therefore voters will be unable to discern whether or not their vote counted in an election. Am I correct on that?

Mr. CUNNINGHAM. I am sorry; repeat that?

Ms. MILLENDER-MCDONALD. Am I correct in saying that because VVPAT is the official ballot record for recount purposes, that if you should need a recount, you cannot go to a reprint to discern whether or not those votes——

Mr. CUNNINGHAM. Right. That is exactly right, Madam. I would submit to you that to reconcile and verify vote totals on an electronic machine, there are better ways to do it in more controlled environments than the election-day environment that I just mentioned. And it is—for instance, when the machine back in the office and other records that are stored in that machine can be printed and otherwise looked at electronically, you know, we work every day on this.

Ms. MILLENDER-MCDONALD. I am sure.

Mr. CUNNINGHAM. We try—that is my job is to try to reconcile those numbers at the end of the day, but trying to maintain this contemporaneous record. And the current state that it is in, and I think we have—I am just saying it is never going to match. And it is only going to fuel this—this fire that voting systems don't work, and I think Ohio has set itself in a very very dangerous situation.

If I may just go on with that, there has been a little talk here about we are only concerned with Federal elections. You know, the least frequent election I run is a Federal election. We need to be very careful that one of the problems that has occurred since the passage of HAVA was it put many State rules and regulations in conflict with the Federal law.

Ms. MILLENDER-MCDONALD. Absolutely.

Mr. CUNNINGHAM. And what we ended up with was these rules apply in a Federal election and these rules apply in a local election. That is a terrible situation. We cannot operate this enterprise with two sets of standards.

Ms. MILLENDER-MCDONALD. I couldn't agree with you more.

Mr. CUNNINGHAM. Please do not think in terms of only Federal elections because it is a very problematic proposition.

Ms. MILLENDER-MCDONALD. Because you know what, sir? In a given election, you have three different laws that you perhaps might have to implement.

Mr. CUNNINGHAM. Could have.

Ms. MILLENDER-MCDONALD. Local, State and Federal. And you know, my hat is off to all of you local elected ones who have to balance between the trenches. It is just really problematic.

Ms. Simons, I will let you close me down because I wanted to go to Mr. Shamos. But I just have a second here for you to comment.

Ms. SIMONS. Yes. I wanted to remind the panel what happened in Carteret County, North Carolina—I believe it was in 2004—where paperless DREs were used and over 4,000 votes were lost. There is a concern about being unable to reprint paper ballots or VVPATs. When you lose votes in a DRE where there is no paper, there is nothing you can do. And in fact there was a statewide election for agricultural commissioner, where the separation between the two candidates was such that the results could have been reversed by those missing votes. And it went to court. The State Board of Elections first tried to hold a vote in just the county. That was thrown out by the court. Then the Board of Elections attempted to hold a statewide vote. That was thrown out by the court because we had no laws to deal with what happens when DREs fail. Finally there were a number of people who submitted subpoenas or petitions saying they voted for one of the candidates; and

based on those submissions, it looked like the judge was going to declare that candidate the winner. So the other candidate conceded, and so that was how the election was decided.

This is not the way to hold elections in this country. This is a problem with DREs, paperless DREs. This was a case of a failure, but there are many other problems too. We haven't even touched upon security problems such as, for example, the risk of somebody malicious getting a job with the vendor or the delivery service and inserting malicious code.

We know that all software is buggy. We don't know, for example, if elections have been wrongly recorded because of buggy software, forget malicious code.

There are so many basic problems that we just have no way of verifying elections that were held on paperless voting machines—we cannot verify them at this point.

The CHAIRMAN. The gentlewoman's time has expired.

Ms. MILLENDER-MCDONALD. This is why the average voter now is just so befuddled over elections.

The CHAIRMAN. And most of us are average voters.

I am pleased to recognize the gentleman from California, Mr. Doolittle, for five minutes.

Mr. DOOLITTLE. Thank you, Mr. Chairman.

Ms. Simons, your written statement said, quote: Unless there is evidence that the VVPBs have been compromised, the paper ballots should be used to determine the election results.

I wanted to ask, what sort of evidence of compromise were you referring to?

Ms. SIMONS. Well, obviously, if you have the kind of mess that Mr. Cunningham talked about, that would raise a lot of concerns. I share his concern about that kind of technology being deployed. We need to have good engineering, we need to have high standards, and we have to hold vendors to high standards. Vendors should not be allowed to produce machines that can create this kind kind of mess.

Mr. DOOLITTLE. Well, they are machines and I notice that machines occasionally make messes.

Ms. SIMONS. You know, sometimes you get what you pay for. You can buy printers that don't jam. You can buy printers that don't have privacy issues. This is not rocket science. These things exist now. These technologies exist now, and I think a question that we have to ask ourselves is how much are we willing to pay for our democracy, you know——

Mr. DOOLITTLE. And our Republic.

Ms. SIMONS. And our Republic; yes, thank you.

Mr. DOOLITTLE. Now I apologize, I should have been here, and I couldn't be here earlier, so I missed the direct testimony. But I think Mr. Cunningham is from Allen County, right? But there was an incident in Cuyahoga County where there was a problem.

I just wondered if you could tell us, Ms. Simons, do you think this evidence of compromise was compromised in the Cuyahoga recount?

Ms. SIMONS. Sir, that is what I was referring to, actually.

Mr. DOOLITTLE. Oh, all right. Do you think the paper trail should have been used as the official ballot in that case? Because that is kind of——

Ms. SIMONS. Well, in that case it is a problem. It is a real problem, just as the Carteret County failure is a real problem. We can see problems with the paperless systems and problems with the systems that have been retrofitted with VVPATs. The underlying issue, which I believe everyone on this panel would agree on, is we need to have well-engineered, well-designed, robust systems. As Mr. Cunningham said, this is sort of like the Model-T. These are first generations and they are failing. That is not good.

Mr. DOOLITTLE. Well, I understand the Model-T analogy, but I don't think the members of this committee and the Congress in general want to throw away hundreds of millions of dollars on the Model-T.

Mr. Dickson, would you like to comment?

Mr. DICKSON. Yes. There were two points. The loss of votes is really, really, a terrible situation.

Mr. DOOLITTLE. Is what, sir?

Mr. DICKSON. The loss of any votes is really a terrible situation. Votes get lost on paper too. The Carteret County voting machine does not meet the current standards. If that county had purchased an accessible voting machine, built to the current standards, that problem would not have happened.

Mr. DICKSON. The Carteret machine, a little red light comes on with no words around, and it says, "This machine is full." There was no explanation in the training for poll workers that said this red light means the machine is full. On the other machine, the machine reads, "Screen full," and will not accept new votes.

Mr. DOOLITTLE. Sir, you said—when are you talking about—are you talking about the one in Cuyahoga County?

Mr. DICKSON. Carteret County in North Carolina where votes were lost on a voting machine. That county administrator wanted to buy new accessible voting equipment, and the purchase of it was delayed because of the commotion about a paper trail. And the problem was created because of the delay.

Mr. DOOLITTLE. Well, I just wonder, in the Cuyahoga County case I understand that the paper trail, which I think Mr. Holt's bill is going to be the thing we go by if there is a conflict—in that case the paper trail lost nearly 10 percent of the votes, so it doesn't seem there would be real problems in that instance at least. Hopefully that would be relatively rare, but in that instance if we went by the paper trail, as the bill called for, there would be problems.

Ms. SIMONS. Actually, there were many problems in that county.I understand there were problems with the DREs; that the redundant memories did not match in about 26 percent of the cases. So if you are going to try to do a verification using the redundant memories, there can be issues.

There were a great many problems, not just involving the VVPATs. This just shows that we need to focus more on technology, on policies and procedures. As Mr. Cunningham said, running an election is a complicated thing, but just because there were problems involving one technology doesn't mean that that technology can't be implemented correctly. Banks deal with money and

paper ballots all the time. Canada holds its Federal election with paper ballots, so does the U.K., and they manage.

Mr. DOOLITTLE. In this case the paper trail didn't solve the problem.

Ms. SIMONS. Because it was badly engineered.

Mr. DOOLITTLE. The point is paper is not the ultimate solution.

The CHAIRMAN. The gentleman's time is expired.

Mr. Brady, you are recognized for 5 minutes.

Mr. BRADY. We are going through as I speak in my city and county in Philadelphia a write-in candidate, as you had, and we are doing that as we speak. We are in court now because the candidate on the machine won. Then they had a paper they could write on, and they are counting the write-in ballots, and that person won, and they are going to decide it in court. So we at least had the opportunity to do that.

I heard you have ways of rectifying or double-checking votes by voting electronically and having a camera. A lot of people don't have good faith in any kind of electronics, and what we are trying to do here is the right thing. We are trying to restore confidence and, most important, trying to restore trust back into our process, and we are trying to figure out the best way to do that.

I understand there is a financial problem, and I understand there is always a financial issue, but like what you said, there is never enough money. You can always find some money to assure democracy, and I subscribe to that.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you.

The Chair recognizes the gentlewoman from California Ms. Lofgren for five minutes.

Ms. LOFGREN. Thank you, Mr. Chairman.

At the conclusion of my first set of questions, Mr. Shamos had described alternative ways to verify the vote. I am wondering if, Mr. Felten, do you have a comment on those proposals, and also Ms. Simons?

Mr. FELTEN. If I recall correctly, he mentioned two mechanisms, one involving a second screen and a video camera. This seems to me more complicated, more expensive than a paper-based verification system and probably not any more trustworthy.

He also mentioned parallel testing, which involves taking the machine aside and holding a simulated election. This is something we discussed in some detail in our research paper, and the bottom line is that that is a worthwhile mechanism, but it is not completely effective, not 100 percent effective at the problem. It raises the bar, makes it more difficult to make a virus, for example, that will evade detection. We should do it, but we should not believe that it is going to entirely fix the problem.

Ms. SIMON. To pick up on Ed's comments, the alternative device that Professor Shamos mentioned makes it very difficult to hold a recount. If you want to have public confidence in elections, one way in which you do that is by audits and recounts. I don't know how you would audit that screen. It seems to me it would have the same problems as these long rolls of paper that Mr. Cunningham showed you, someone to sit in front and say, this one voted here, and this one voted there.

Ms. LOFGREN. Mr. Smith, do you have a comment on it? I cut you off, Barbara. I didn't mean to.

Ms. SIMONS. May I finish? The best way to count things is the way you count money, you sort it into piles, and you count each pile, and that can be transparently and with a TV camera watching a count as a way in getting confidence in the results.

Regarding parallel testing, I think we agree parallel testing is a good thing to do. But there is a big "what if," and that "what if" is: What if you find a problem with the parallel testing? Are you going to go back and rerun the election? As we saw in Carteret County, that raises enormous legal and technical problems.

Ms. LOFGREN. Mr. Smith.

Mr. SMITH. I would like to speak from the complexity of the operation that you are trying to bring about. One of the things we have got in Georgia is a more simple format, I think, for running the election because we do not have voter-verifiable paper trail. One of the issues—I was actually charged with running the manual recount, so I have some experience with that, too. I wanted to see it being done because it is being talked about in our State.

One of the concerns I have, and I think we all should look back to, is who are the people putting this stuff into operation on election day? It is typical. We have done things, you see it. We have part-time people who are volunteers who really try to do things, but they have gotten up at 4:00 in the morning, 5:00 in the morning. They have to open the machines up, do all the other things.

In Ohio with the VVPAT for Cuyahoga County, they had to do other things that we didn't have to do. They go through the logic and accuracy testing essentially right there. They enter the machines, they start them up, they do everything. They bring the memory cards. Part of the problem was the memory cards weren't seated properly. That was a problem. But the other thing is they had to be responsible for these printers. In some cases they put the paper in backwards.

Ms. LOFGREN. Let me explore that, because I am taking as a given that we are not going to completely change the way America holds elections, I think that is true. And I can remember voting when I was still at my parents' house, and you go down to the corner, and Mrs. Lucky, who always ran it, and it is retirees and people that volunteer, and it is a wonderful thing, but that is the given.

A lot of States have these verifiable systems, California among them. Ms. Simons, has any of them come up with a system that actually works better than that silly tape that we have seen?

Ms. SIMONS. I think precinct-based optical scan systems are excellent. That gives the voter a chance to check for overvotes and the absence votes. You put your ballot through the scanner, and it tells you if there is a problem with it. Recounts and audits are relatively easy. The voter verifies the ballot by definition, because the voter can look at it.

There are ways for blind voters to verify an optical scanballot. One possibility is the use of a hand-held device that reads the ballot for a blind voter. We know that this technology exists. Another is to allow blind voters to use tactile ballots where they insert the blank ballot into a sleeve envelope that is marked. The sleeve has

holes that allow a blind voter to mark the ballots. There is also a system being marketed which allows a blind voter to verify his or her ballot with a vibrating device.

Ms. LOFGREN. I see my time has expired, but I would just like to note that I think we may have in the future some other way to verify, but I just ask Mr. Holt to put me on his bill because I think we need to have some in between on this. [Applause.]

The CHAIRMAN. No demonstrations.

I am now pleased to recognize Mr. Holt for five minutes.

Mr. HOLT. Thank you, Mr. Chairman.

My questioning will be along a couple of lines. First of all, Mr. Shamos, I am sorry I didn't have the exact transcript here, but said something or other you hate to see us outlaw an entire category of machines. This legislation doesn't outlaw any particular kind of voting system except unverifiable ones.

And you said further, I think, that scare tactics by a minority, you hate to see that disrupt the whole process. The Brennan Center for Justice of New York University Law School conducted a study with very distinguished people, Ron Rivest from MIT, Howard Schmidt, an administration and corporate security expert, and a number of others; and said it found, quote, all three major types of voting systems have significant security and reliability vulnerabilities that pose a real danger to the integrity of national, State and local elections.

The League of Women Voters, not a scary minority, says they support, quote, only voting systems that are designed so that they employ a voter-verifiable paper ballot or other paper record, said paper being the official record of the voter's intent.

The report of the Carter-Baker Commission similarly called for a voter-verified paper record, random audits and so forth.

Mr. Chairman, I would like to ask that the Brennan Center report, the statement of the National League of Women Voters and the Carter-Baker report be made a part of the record.

The CHAIRMAN. Without objection, so ordered.

Mr. HOLT. Thank you. I want to make the point that a number of organizations, very responsible organizations with computer scientists involved and so forth, have taken a look at this matter, and we would do well to take a look at that.

Ms. Simons, I would appreciate it if you would say a little bit more about ACM and the subcommittee that is looking at this.

Then also what I would like the witnesses to comment on, as Mr. Dickson recounts and Mr. Smith and others, votes can be lost in a lot of ways. They can be lost through manipulating the registration list, intimidating voters. There are a lot of things that we need to address: Restricting accessibility at polling places or in the polling booth; memory cards may not be seated properly; we may not recognize that the memory is full before election day is over; and paper records, Mr. Doolittle, might be illegible or torn or otherwise difficult to use. But it has been determined at least as often that redundant electronic memories show that there are problems with purely electronic memory.

So what I would like to ask of the witnesses is would you prefer to have a system where there is no possible way of recovering what happened, in other words, where the electronic vote, for whatever

reason, a poorly seated memory card or something else, is wrong, and there is no possible way of recovering it; or, as Ms. Simons points out, a well-designed system with a paper audit trail where there is at least a reasonable chance of being able to recapture, recover what the voters' intentions were?

So I would be happy to have a quick comment from the witnesses, beginning with Ms. Simons.

Ms. SIMONS. You asked me about ACM. It is an 80,000-member professional society of computer professionals. Like the APS, (the American Physical Society), the ACM is the premier computing society, I would say, in this country.

The statement that I referred to, which is in my written testimony, was voted on by ACM Council, which is the elected policy making body of ACM. But they did something unusual, not typical for ACM. The statement was put on the Web site for members to vote on. Of those who voted, 95 percent supported the statement. Of the 5 percent who did not support the statement, roughly half, based on written comments, objected to the fact that it wasn't broad enough, that it didn't discuss usability issues as well.

So I would say obviously you never get 100 percent agreement, but in this case we are pretty close to consensus, at least within ACM.

The CHAIRMAN. The gentleman's time has expired. Make brief comments, please. Mr. Shamos, first.

Mr. SHAMOS. I want to respond to a couple of things. I actually didn't make a comment about scare tactics, although I believe there was another member of the panel that did. I just said I don't think we should appeal to emotion on this issue.

I agree that H.R. 550 does not expressly outlaw any particular type of voting equipment. My point was that the practical effect of it is that it outlaws DRE machines, and the reason it outlaws DRE machines is there is no current machine on the market that meets the requirement of the bill and that is usable in individual States along with their requirements.

For example, in Pennsylvania there is popular call for a paper trail machine. Four vendors have come to Pennsylvania with their paper trail machine. Not a single one has been able to simultaneously offer a paper trail and meet Pennsylvania's statutory and constitutional requirements. So we can't have one even if we want one. The technology is just not there yet.

The CHAIRMAN. I think Mr. Felten had a comment.

Mr. FELTEN. The key issue, I think, is resiliency; things go wrong, people make mistakes, and we need to have a system we can trust even when things do go wrong. The combination of paper plus electronic record is more resilient than either one would be alone, and that, I think, is the strongest argument for having a paper-based verification system.

Mr. EHLERS. I think Mr. Cunningham has the last answer.

Mr. CUNNINGHAM. I just wanted to make the point to everybody that my experience is most votes are lost due to voter error, not machine error, not election official error. I don't know if you looked at my resume, but I have about 20 years in the printing business, and I have been around a lot of printing machines and copy ma-

chines, and I can assure you anything you put paper through will jam at some point in time.

E-voting, I want to say to you, I truly believe that in the long-term interest of this country—we are still voting the same way we did 150 years ago, as you mentioned, Ms. Lofgren, down to your little poll at the corner and precinct. Our society has changed. It is mobile, moving. The ability to incorporate the vote centers as Scott Doyle in Colorado has been working with as a convenience to voters, those types of concepts are based on electronic voting.

Let's not throw the baby out with the bath water here. I think, Mr. Brady, what is doing more damage to voter confidence, quite frankly, is people like your distinguished colleague Mr. Conyers publishing reports about the election in Ohio that are factless and baseless; none of the accusations have been proved.

We have got to quit this. We have got to get this conversation back to an honest debate about, as I think the whole panel has said, how do we work together and move this thing forward and quit this sky is falling kind of thing. I think elections, because given the magnitude of them—and I have seen now 9 years' worth of them, two Presidential, couple of gubernatorials—given what could happen and the magnitude of the task, they are running pretty darn good in this country, and I know people all over the country like myself and Mr. Smith that are darn proud they are involved in it. And the net effect is we are going to begin to drive those people out of this, which is going to make the system more vulnerable than you ever imagined.

Ms. MILLENDER-MCDONALD. Mr. Cunningham, I sure hope that is accurate, what you have said, because the voter is not there yet. Even though you folks are and your experts, the voter is not there yet. And that is the ultimate one that we must bring trust, security to bear.

I would like for you to get for me whatever documentation you have that suggests voter error is more than a paper error. If you have that type of verification of that statement you made, I would like to have it.

Mr. CUNNINGHAM. My point was that most voting error is voter error.

The CHAIRMAN. I thank you for your comments. That is a good wrap-up. We are going to have votes in just a few moments, and I would just like to make a few closing comments.

First of all, I thank each and every one of you for being here in the audience as well as at the witness table. You have contributed immensely to this very important issue.

There is our votes.

I recognize very clearly, since I have served at the local level, the state legislature and now here, that the states have an important role, local governments have an important role, and the federal government has an important role.

We often say here that the states are the experimental apparatus that tests ideas, and then the federal government should select from the best of what the states have discovered. We did not take the time to do that in HAVA, and I think that was a mistake. We also did not take the time to first set the standards clearly and then allow manufacturers to develop equipment to meet those

standards. And I think that was a fatal flaw which has, I believe, created much of the uncertainty that we have.

I agree totally with the statement someone made: Never buy the first model of anything. I bought the first model of one automobile just because it precisely fit my needs, it was a good manufacturer; a bad mistake, and I was frankly relieved when the car eventually got totaled and I got the insurance value because I probably could never have sold it.

We have to recognize that there is a lot of work to be done here yet, and the American public's confidence will return because we will build a better system.

Finally, I want to comment that I always look at two aspects here. We want to assure every voter that their vote will be counted, be counted accurately, and that the system will work that way. There is a second factor we must remember, and that gets back to the viruses and other issues. We also have to assure every voter that not only will the vote be counted, but it will not be negated or diluted by other people voting fraudulently or performing fraudulent acts such as viruses, throwing ballot boxes away and so forth. I want to make sure every voter is assured of both of those—an accurate count of their vote and an assurance that no one else is going to negate it through illegal activity.

So I am concentrating on those two not just in this particular issue, but in other issues such as the photo ID bill that we passed through the House a week ago, which I think will also help.

Thank you very, very much. You have been an outstanding panel. I appreciate all that you have done. We do have to go vote, and I have a few things to read here. I ask unanimous consent that Members and witnesses have seven calendar days to submit material for the record, including additional questions of the witnesses, and for those statements and materials to be entered into the appropriate place in the record. And I assume if we send you written questions, you will respond to those.

Without objection the material will be so entered.

The CHAIRMAN. I ask unanimous consent that staff be authorized to make technical and conforming changes on all matters considered by the committee at today's hearing. Without objection, so ordered.

Ms. Millender-McDonald.

Ms. MILLENDER-MCDONALD. I just wanted to concur with you. I have served on the local, State and Federal level, and I do think that we need to revisit HAVA because it was more or less geared for the Federal. And we appreciate all of those who have come today, those who serve on both the local, State and Federal. Thank you, Mr. Chairman.

The CHAIRMAN. Thank you.

Having completed our business for today and for this hearing, the committee is hereby adjourned.

[Whereupon, at 12:23 p.m., the committee was adjourned.]



Resolution adopted by the League of Women Voters of the United States 2006 National Convention.

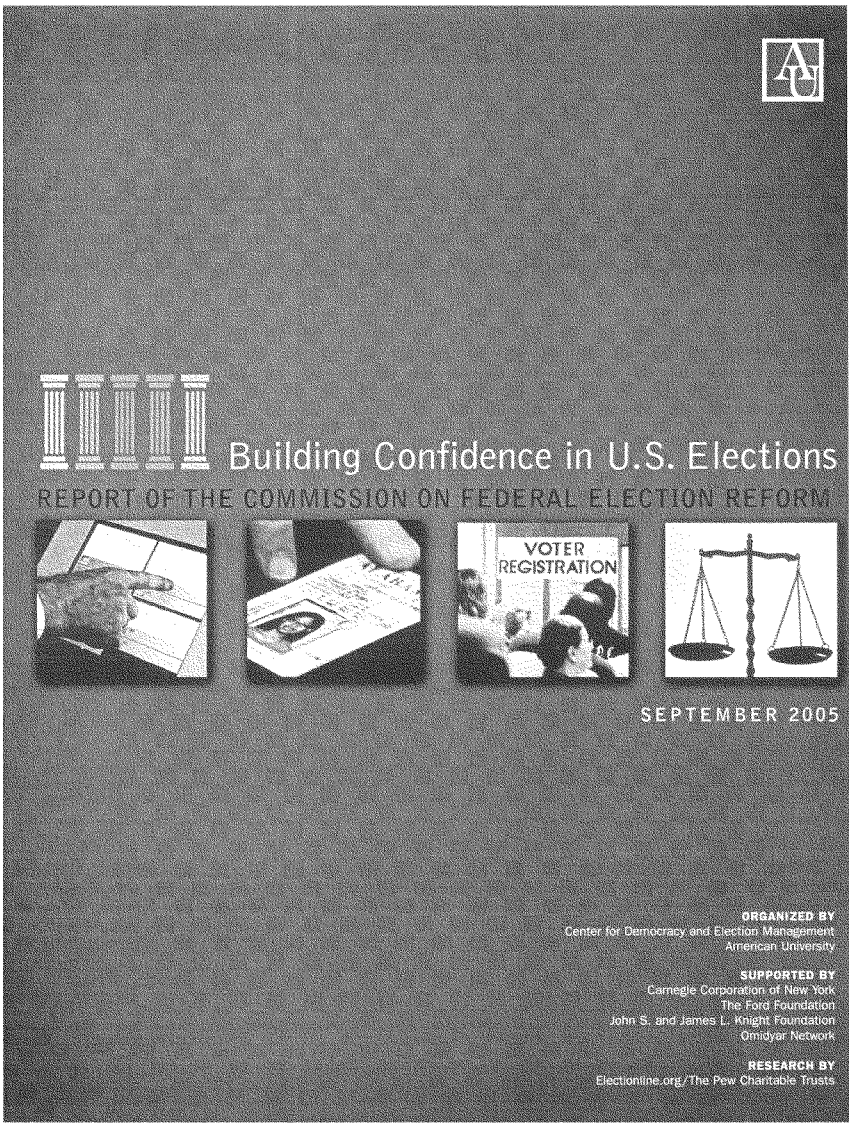
Whereas: Some LWVs have had difficulty applying the SARA Resolution (Secure, Accurate, Recountable and Accessible) passed at the last Convention, and

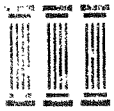
Whereas: Paperless electronic voting systems are not inherently secure, can malfunction, and do not provide a recountable audit trail,

Therefore be it resolved that:

The position on the Citizens' Right to Vote be interpreted to affirm that LWVUS supports only voting systems that are designed so that:

1. they employ a voter-verifiable paper ballot or other paper record, said paper being the official record of the voter's intent; and
2. the voter can verify, either by eye or with the aid of suitable devices for those who have impaired vision, that the paper ballot/record accurately reflects his or her intent; and
3. such verification takes place while the voter is still in the process of voting; and
4. the paper ballot/record is used for audits and recounts; and
5. the vote totals can be verified by an independent hand count of the paper ballot/record; and
6. routine audits of the paper ballot/record in randomly selected precincts can be conducted in every election, and the results published by the jurisdiction.


Building Confidence in U.S. Elections
REPORT OF THE COMMISSION ON FEDERAL ELECTION REFORM
VOTER REGISTRATION
SEPTEMBER 2005
ORGANIZED BY
Center for Democracy and Election Management
American University
SUPPORTED BY
Carnegie Corporation of New York
The Ford Foundation
John S. and James L. Knight Foundation
Omidyar Network
RESEARCH BY
Electionline.org/The Pew Charitable Trusts



Building Confidence in U.S. Elections

REPORT OF THE COMMISSION ON FEDERAL ELECTION REFORM

SEPTEMBER 2005

ORGANIZED BY
Center for Democracy and Election Management
American University

SUPPORTED BY
Carnegie Corporation of New York
The Ford Foundation
John S. and James L. Knight Foundation
Omidyar Network

RESEARCH BY
Electionline.org/The Pew Charitable Trusts

Building Confidence in U.S. Elections

REPORT OF THE COMMISSION ON FEDERAL ELECTION REFORM

Table of Contents

Letter from the Co-Chairs ... ii

Preface by the Executive Director ... iii

Executive Summary ... iv

1: Goals and Challenges of Election Reform ... 1

1.1 Help America Vote Act: Strengths and Limitations ... 2

1.2 Learning from the World ... 5

1.3 Transforming the Electoral System – Five Pillars ... 6

1.4 Urgency of Reform ... 7

2: Voter Registration and Identification ... 9

2.1 Uniformity Within States – Top-Down Registration Systems ... 10

2.2 Interoperability Among States ... 12

2.3 Provisional Ballots ... 15

2.4 Communicating Registration Information ... 16

2.5 Voter Identification ... 18

2.6 Quality in Voter Registration Lists ... 22

3: Voting Technology ... 25

3.1 Voting Machines ... 25

3.2 Audits ... 28

3.3 Security for Voting Systems ... 28

3.4 Internet Voting ... 32

4: Expanding Access to Elections ... 33

4.1 Assured Access to Elections ... 33

4.2 Vote by Mail ... 35

4.3 Vote Centers ... 36

4.4 Military and Overseas Voting ... 37

4.5 Access for Voters with Disabilities ... 39

4.6 Re-Enfranchisement of Ex-Felons ... 40

4.7 Voter and Civic Education ... 41

5: Improving Ballot Integrity ... 45

5.1 Investigation and Prosecution of Election Fraud ... 45

5.2 Absentee Ballot and Voter Registration Fraud ... 46

6: Election Administration ... 49

6.1 Institutions ... 49

6.2 Poll Worker Recruitment ... 54

6.3 Polling Station Operations ... 56

6.4 Research on Election Management ... 57

6.5 Cost of Elections ... 59

7: Responsible Media Coverage ... 61

7.1 Media Access for Candidates ... 61

7.2 Media Projections of Election Results ... 62

8: Election Observation ... 65

9: Presidential Primary and Post-Election Schedules ... 67

9.1 Presidential Primary Schedule ... 67

9.2 Post-Election Timeline ... 68

Conclusion ... 69

Appendix ... 71
Estimated Costs of Recommended Improvements

Endnotes ... 72

Summary of Recommendations ... 79

Additional Statements ... 88

About the Commission on Federal Election Reform ... 92

LETTER FROM THE CO-CHAIRS

Elections are the heart of democracy. They are the instrument for the people to choose leaders and hold them accountable. At the same time, elections are a core public function upon which all other government responsibilities depend. If elections are defective, the entire democratic system is at risk.

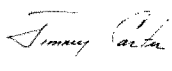
Americans are losing confidence in the fairness of elections, and while we do not face a crisis today, we need to address the problems of our electoral system.

Our Commission on Federal Election Reform was formed to recommend ways to raise confidence in the electoral system. Many Americans thought that one report — the Carter-Ford Commission — and one law — the Help America Vote Act of 2002 (HAVA) — would be enough to fix the system. It isn't. In this report, we seek to build on the historic achievement of HAVA and put forward a bold set of proposals to modernize our electoral system.

Some Americans will prefer some of our proposals to others. Indeed, while all of the Commission members endorse the judgments and general policy thrust of the report in its entirety, they do not necessarily support every word and recommendation. Benefitting from Commission members with diverse perspectives, we have proposed, for example, a formula for transcending the sterile debate between integrity and access. Twenty-four states now require identification for voters, with some systems likely to restrict registration. We are recommending a photo ID system for voters designed to increase registration with a more affirmative and aggressive role for states in finding new voters and providing free IDs for those without driver's licenses. The formula we recommend will result in both more integrity and more access. A few of our members have expressed an alternative view of this issue.

Still, our entire Commission is united in the view that electoral reform is essential and that our recommended package of proposals represents the best way to modernize our electoral system. We urge all Americans, including the legislative and executive branches of government at all levels, to recognize the urgency of election reform and to seriously consider the comprehensive approach outlined herein.

We present this report because we believe the time for acting to improve our election system is now.



Jimmy Carter



James A. Baker, III

Co-Chairs of the Commission on Federal Election Reform

PREFACE BY THE EXECUTIVE DIRECTOR

Polls indicate that many Americans lack confidence in the electoral system, but the political parties are so divided that serious electoral reform is unlikely without a strong bipartisan voice. Our country therefore owes a great debt to former President Jimmy Carter and former Secretary of State James A. Baker, III for leading this Commission and forging a plan for election reform.

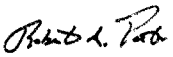
To build confidence, the Commission recommends a modern electoral system built on five pillars: (1) a universal and up-to-date registration list, accessible to the public; (2) a uniform voter identification system that is implemented in a way that increases, not impedes, participation; (3) measures to enhance ballot integrity and voter access; (4) a voter-verifiable paper trail and improved security of voting systems; and (5) electoral institutions that are impartial, professional, and independent. Democrats, Republicans, and Independents tend to prefer different elements of this package, but President Carter and Secretary Baker drew strength rather than stalemate from the diverse perspectives in fashioning an approach that is greater than the sum of these parts.

Our Commission was fortunate to have an outstanding staff and academic advisors, and we have benefited from advice by Members of Congress and staff, election officials, and representatives of a wide range of non-governmental organizations devoted to improving our democracy. See our website for a list of advisors and the studies and testimony: www.american.edu/Carter-Baker.

We acknowledge the support of many at the end of this report, but let me identify here a few people whose work was crucial to the Commission: Daniel Calingaert, the Associate Director of American University's Center for Democracy and Election Management, Doug Chapin of Electionline.org, John Williams, Senior Advisor to Secretary Baker, Kay Stimson, Media Liaison, and Murray Gormly, Administrative Coordinator. The Commission was organized by American University's Center for Democracy and Election Management. We are also grateful to the James A. Baker III Institute for Public Policy of Rice University and The Carter Center for hosting the other two meetings.

Finally, the Commission could not have accomplished its goal without the generosity of its funders and the advice and support of the following individuals: Geri Mannion of the Carnegie Corporation; Thomasina Williams of the Ford Foundation; Julie Kohler of the John S. and James L. Knight Foundation; Dena Jones of Omidyar Network, and The Pew Charitable Trusts.

At AU's Center for Democracy and Election Management, we view this Commission as a major step toward developing the educational foundation for students, professionals, and the public to deepen our understanding of democracy and elections in the United States and the world.



Robert A. Pastor,
Executive Director

EXECUTIVE SUMMARY

Building confidence in U.S. elections is central to our nation's democracy. At a time when there is growing skepticism with our electoral system, the Commission believes that a bold new approach is essential. The Commission envisions a system that makes Americans proud of themselves as citizens and of democracy in the United States. We should have an electoral system where registering to vote is convenient, voting is efficient and pleasant, voting machines work properly, fraud is deterred, and disputes are handled fairly and expeditiously.

This report represents a comprehensive proposal for modernizing our electoral system. We propose to construct the new edifice for elections on five pillars:

First, we propose a universal voter registration system in which the states, not local jurisdictions, are responsible for the accuracy and quality of the voter lists. Additionally, we propose that the U.S. Election Assistance Commission (EAC) develop a mechanism to connect all states' list. These top-down and interoperable registration lists will, if implemented successfully, eliminate the vast majority of complaints currently leveled against the election system. States will retain control over their registration list, but a distributed database can remove interstate duplicates and help states to maintain an up-to-date, fully accurate registration list. This would mean people would need to register only once in their lifetime, and it would be easy to update their registration information when they move. We also propose that all states establish uniform procedures for counting provisional ballots, and many members recommend that the ballots should be counted if the citizen has voted in the correct jurisdiction.

Second, to make sure that a person arriving at a polling site is the same one who is named on the list, we propose a uniform system of voter identification based on the "REAL ID card" or an equivalent for people without a drivers license. To prevent the ID from being a barrier to voting, we recommend that states use the registration and ID process to enfranchise more voters than ever. States should play an affirmative role in reaching out to non-drivers by providing more offices, including mobile ones, to register voters and provide photo IDs free of charge. There is likely to be less discrimination against minorities if there is a single, uniform ID, than if poll workers can apply multiple standards. In addition, we suggest procedural and institutional safeguards to make sure that the rights of citizens are not abused and that voters will not be disenfranchised because of an ID requirement. We also propose that voters who do not have a photo ID during a transitional period receive a provisional ballot that would be counted if their signature is verified.

Third, we propose measures that will increase voting participation by having the states assume greater responsibility to register citizens, make voting more convenient, and offer more information on registration lists and voting. States should allow experimentation with voting centers. We propose ways to facilitate voting by overseas military and civilians and ways to make sure that people with disabilities have full access to voting. In addition, we ask the states to allow for restoration of voting rights for ex-felons (other than individuals convicted of capital crimes or registered sex offenders) when they have fully served their sentence. We also identify several voter and civic education programs that could increase participation and inform voters, for example, by providing information on candidates and the voting process to citizens before the election. States and local jurisdictions should use Web sites, toll-free numbers, and other means to inform citizens about their registration status and the location of their precinct.

To improve ballot integrity, we propose that federal, state, and local prosecutors issue public reports on their investigations of election fraud, and we recommend federal legislation to deter or prosecute systemic efforts to deceive or intimidate voters. States should not discourage legal voter registration or get-out-the-vote activities, but they need to do more to prevent voter registration and absentee ballot fraud.

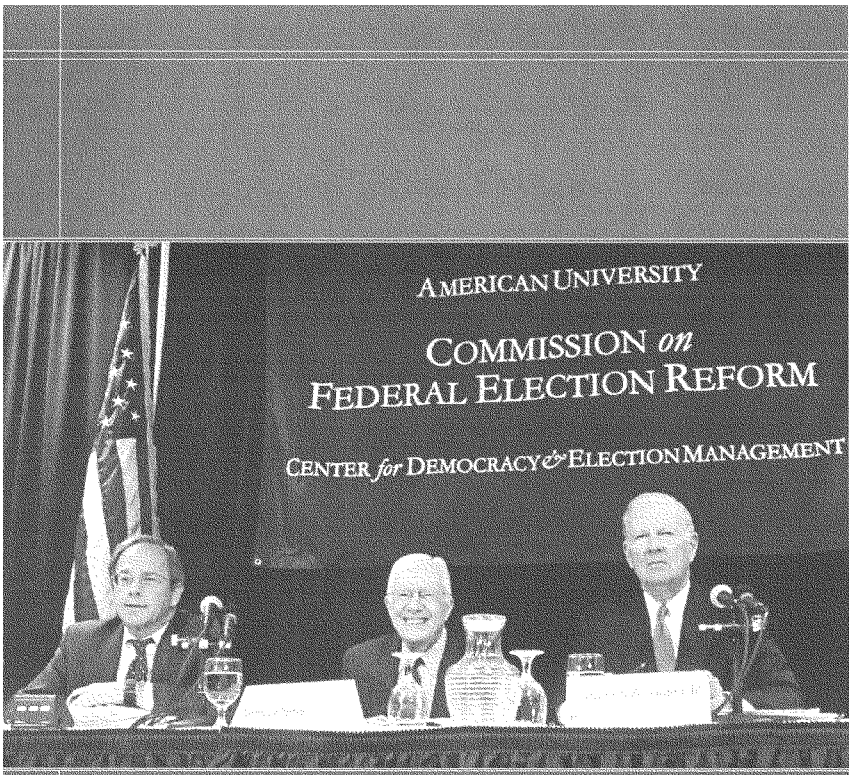
Fourth, we propose ways to give confidence to voters using electronic voting machines that their votes will be counted accurately. We call for an auditable backup on paper at this time, but we recognize the possibility of alternative technologies to audit those machines in the future. We encourage independent testing of voting systems (to include voting machines and software source code) under EAC supervision.

Finally, we recommend strengthening and restructuring the system by which elections have been administered in our country. We propose that the EAC and state election management bodies be reconstituted on a nonpartisan basis to become more independent and effective. We cannot build confidence in elections if secretaries of state responsible for certifying votes are simultaneously chairing political campaigns, and the EAC cannot undertake the additional responsibilities recommended by this report, including critical research, without gaining additional funds and support. Polling stations should be organized to reduce the chances of long lines; they should maintain "log-books" on Election Day to record complaints; and they need electronic poll-books to help voters find their correct precinct. HAVA should be fully funded and implemented by 2006.

The Commission puts forward 87 specific recommendations. Here are a few of the others:

- We propose that the media improve coverage of elections by providing at least five minutes of candidate discourse every night in the month preceding the election.
- We ask news organizations to voluntarily refrain from projecting presidential election results until polls close in the 48 contiguous states.
- We request that all of the states provide unrestricted access to all legitimate domestic and international election observers, as we insist of other countries, but only one state currently permits; and
- We propose changing the presidential primary schedule by creating four regional primaries.

Election reform is neither easy nor inexpensive. Nor can we succeed if we think of providing funds on a one-time basis. We need to view the administration of elections as a continuing challenge, which requires the highest priority of our citizens and our government.



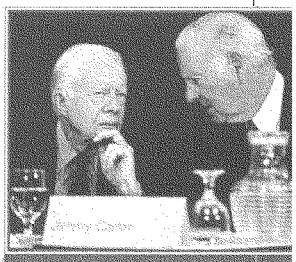
(American University Photo/Jeff Watts)

1. Goals and Challenges of Election Reform

The vigor of American democracy rests on the vote of each citizen. Only when citizens can freely and privately exercise their right to vote and have their vote recorded correctly can they hold their leaders accountable. Democracy is endangered when people believe that their votes do not matter or are not counted correctly.

Much has happened since November 2000, when many Americans first recognized that their electoral system had serious problems with flawed voter registration lists, obsolete voting machines, poorly designed ballots, and inadequate procedures for interpreting disputed votes. Congress and the President, Democrats and Republicans, responded with a truly historic initiative – the Help America Vote Act of 2002 (HAVA), the first comprehensive federal law in our nation's history on electoral administration. The law represents a significant step forward, but it falls short of fully modernizing our electoral system.

On the eve of the November 2004 election, a *New York Times* poll reported that only one-third of the American people said that they had a lot of confidence that their votes would be counted properly, and 29 percent said they were very or somewhat concerned that they would encounter problems at the polls. Aware of this unease, the U.S. Department of Justice deployed 1,090 election observers — more than three times the number sent in 2000.[1] After the election, a minority of Americans — only 48 percent — said they were very confident that the votes cast across the country were accurately counted, according to a Pew Research Center survey. Thirty-seven percent had doubts (somewhat confident), and 14 percent were not confident that the votes were accurately counted.[2]



Former President Jimmy Carter and former Secretary of State James A. Baker III. (AP Photo/Charles Dharapak)

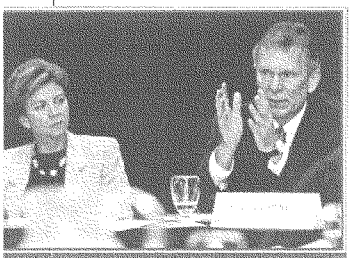
With a strong desire to contribute to building confidence in our electoral process, this Commission came together to analyze the state of the electoral system, to assess HAVA's implementation, and to offer recommendations for further improvement. Public confidence in the electoral system is critical for our nation's democracy. Little can undermine democracy more than a widespread belief among the people that elections are neither fair nor legitimate. We believe that further important improvements are necessary to remove any doubts about the electoral process and to help Americans look upon the process of casting their ballot as an inspiring experience — not an ordeal.

We address this report to the American people and to the President, Congress, U.S. Election Assistance Commission, states, election administrators, and the media. Our recommendations aim both to increase voter participation and to assure the integrity of the electoral system. To achieve those goals, we need an accurate list of registered voters, adequate voter identification, voting technology that precisely records and tabulates votes and is subject to verification, and capable, fair, and nonpartisan election administration.

While each state will retain fundamental control over its electoral system, the federal government should seek to ensure that all qualified voters have an equal opportunity to exercise their right to vote. This will require greater uniformity of some voting requirements and registration lists that are accurate and compatible among states. Greater uniformity is also needed within states on some voting rules and procedures. The federal government should fund research and development of voting technology that will make the counting of votes more transparent, accurate, and verifiable.

1.1 HELP AMERICA VOTE ACT: STRENGTHS AND LIMITATIONS

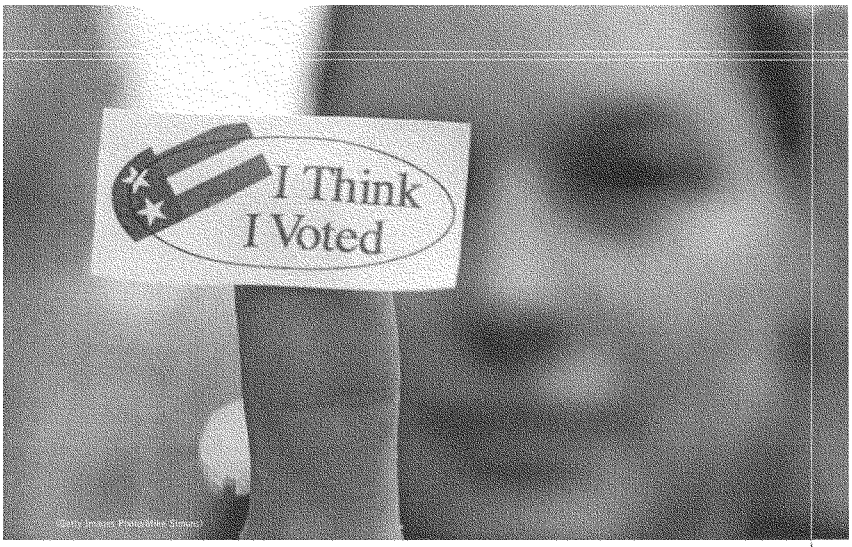
The Help America Vote Act of 2002 (HAVA) established numerous federal requirements for state and local election administration in exchange for a promise of $3.97 billion in federal funding, of which approximately $3.1 billion has been appropriated to date. These requirements reflected a national consensus on the general outline of reform, best represented by the 2001 report of the National Commission on Federal Election Reform, co-chaired by former Presidents Jimmy Carter and Gerald Ford. HAVA's mandates were adopted as part of a compromise between the parties on the divisive issue of access to the ballot (largely championed by Democrats and their allies) versus protecting the integrity of the electoral process (generally favored by Republicans and their supporters).



Commissioners Susan Molinari and Tom Daschle
(American University Photo/Willard Matewson)

Under this compromise, described by its sponsors as making it "easier to vote and harder to cheat," HAVA sought to lower barriers to voting while establishing somewhat tighter controls on registration and voter identification. Consequently, HAVA's mandates focused on four major requirements: (1) statewide computerized voter lists; (2) voter ID for individuals who register by mail but do not provide it when registering; (3) provisional ballots for voters whose names are missing from the registration rolls on Election Day; and (4) measures to make voting more accessible for voters with disabilities. The main provisions of HAVA are as follows:

- Voter registration lists, which were typically maintained at the local level, are now being consolidated into statewide voter databases.
- All states are required to provide provisional ballots on Election Day to citizens who believe they are registered but whose names do not appear on the registration lists.
- HAVA provides federal funding — for the first time — to create statewide voter databases and to replace old voting machines.
- All voting systems used in federal elections are required to meet minimum standards for voter verification of ballots, accessibility for voters with disabilities and language minorities, notification of over-votes, and auditing procedures.



- HAVA calls for the testing and certification of voting systems as a way to make sure they operate properly on Election Day.

- The U.S. Election Assistance Commission (EAC) was created to disburse federal funds, develop guidelines for voting systems, serve as a clearinghouse of information to improve election administration throughout the country, and study and report on how to make elections more accessible and accurate.

Under HAVA, states are required to complete their statewide voter databases by January 1, 2006, and some expenditures of HAVA funds will extend well beyond that date. Our Commission therefore calls for full implementation and full funding of HAVA.

The first presidential election after HAVA became law — on November 2, 2004 — brought to light as many problems as in 2000, if not more. HAVA, which will take years to be fully implemented, was not responsible for most of the complaints. Instead, voters were discouraged or prevented from voting by the failure of election offices to process voter registration applications or to mail absentee ballots in time, and by the poor service and long lines at polling stations in a number of states. There were also reports of improper requests for voter ID and of voter intimidation and suppression tactics. Concerns were raised about partisan purges of voter registration lists and about deliberate failures to deliver voter registration applications to election authorities. Moreover, computer malfunctions impugned election results for at least one race, and different procedures for counting provisional ballots within and between states led to legal challenges and political protests. Had the margin of victory for the presidential contest been narrower, the lengthy dispute that followed the 2000 election could have been repeated.

The November 2004 elections also showed that irregularities and fraud still occur. In Washington, for example, where Christine Gregoire was elected governor by a 129-vote margin, the elections superintendent of King County testified during a subsequent unsuccessful election challenge that ineligible ex-felons had voted and that votes had been cast in the names of the dead. However, the judge accepted Gregoire's victory because with the exception of four ex-felons who admitted to voting for Dino Rossi, the authorities could not determine for whom the other illegal votes were cast. In Milwaukee, Wisconsin, investigators said they found clear evidence of fraud, including more than 200 cases of felons voting illegally and more than 100 people who voted twice, used fake names or false addresses, or voted in the name of a dead person. Moreover, there were 4,500 more votes cast than voters listed.[3] One potential source of election fraud arises from inactive or ineligible voters left on voter registration lists. By one estimate, for example, there were over 181,000 dead people listed on the voter rolls in six swing states in the November 2004 elections, including almost 65,000 dead people listed on the voter rolls in Florida.[4]



Commissioners Bob Michel and Shirley Mattson (American University Photo/Willard Harraden)

Some of these problems may be addressed by the full implementation of HAVA, but it is clear that others will not. Due to vague mandates on provisional voting and identification cards, counties and states applied different standards. This led to a significant proliferation of legal challenges. A closer presidential election likely would have brought an avalanche of litigation. HAVA does not address interoperable registration lists among states, and it is also vague as to whether states should create a top-down, state-controlled registration list or a bottom-up list controlled by local election administrators. The weak structure of the U.S. Election Assistance Commission, a product of a HAVA compromise, has stymied its ability to be clear or authoritative on almost any subject, even on whether to verify electronic machine votes with paper ballots. Thus, there is a compelling need for further election reform that builds on HAVA.

One of the most important laws on the right of Americans to vote is the Voting Rights Act of 1965. Key provisions of the Act are due to expire in 2007. These include the language provision (Section 203), which requires jurisdictions to provide voting materials in minority languages in areas where language minority groups make up a significant portion of the population, and the pre-clearance provision (Section 5), which requires federal pre-clearance for all changes to voting rules or procedures made by specified jurisdictions with a history of voter discrimination. Our Commission believes this Act is of the utmost importance.

Recommendations on the Help America Vote Act and the Voting Rights Act

1.1.1 The Help America Vote Act should be fully implemented by 2006, as mandated by the law, and fully funded.

1.1.2 The Commission urges that the Voting Rights Act be vigorously enforced and that Congress and the President seriously consider reauthorizing those provisions of the Act that are due to expire in 2007.

1.2 LEARNING FROM THE WORLD

In its deliberations, our Commission considered the best practices of election systems around the world. Many other democracies achieve significantly higher levels of voter participation due, in part, to more effective voter registration. Election authorities take the initiative to contact and register voters and conduct audits of voter registration lists to assure that they are accurate. In addition, voter registration in many countries is often tied directly to a voter ID, so that voter identification can enhance ballot integrity without raising barriers to voting. Voters in nearly 100 democracies use a photo identification card without fear of infringement on their rights.[5]

Nonpartisan election administration has also proved effective abroad. Over the past three decades, election management institutions have evolved in many other democracies. Governments had previously conducted elections, but as concern was raised that they might give advantage to incumbents, independent election commissions were formed. Initially, election commissioners in other countries frequently represented political parties, but they often stalemated or reached agreement with each other at the public's expense. This explains why the trend in the world is toward independent election commissions composed of nonpartisan officials, who serve like judges, independently of the executive or legislative branches (see Table 5 on page 52). Political party representatives can observe deliberations on these commissions but not vote on decisions. Nonpartisan election officials are generally regarded as fair arbiters of the electoral process who make their best efforts to administer elections impartially and effectively.



Mexico's Federal Electoral Institute (IFE)
(AP Photo/Marco Ugarte)

1.3 TRANSFORMING THE ELECTORAL SYSTEM – FIVE PILLARS

The recommendations of our Commission on Federal Election Reform aim both to increase voter participation and to assure the integrity of the electoral system. To accomplish these goals, the electoral system we envision should be constructed on the following five sturdy pillars:

Voter registration that is convenient for voters to complete and even simpler to renew and that produces complete, accurate, and valid lists of citizens who are eligible to vote;

Voter identification, tied directly to voter registration, that enhances ballot integrity without introducing new barriers to voting, including the casting and counting of ballots;

Measures to encourage and achieve the greatest possible participation in elections by enabling all eligible voters to have an equal opportunity to vote and have their votes counted;

Voting machines that tabulate voter preferences accurately and transparently, minimize under- and over-votes, and allow for verifiability and full recounts; and

Fair, impartial and effective election administration.

An electoral system built on these pillars will give confidence to all citizens and will contribute to high voter participation. The electoral system should also be designed to reduce the possibility or opportunity for litigation before, and especially after, an election. Citizens should be confident that the results of the election reflect their decision, not a litigated outcome determined by lawyers and judges. This is achieved by clear and unambiguous rules for the conduct of the election established well in advance of Election Day.



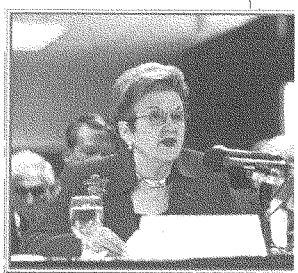
Common Cause President Chellie Pingree (American University Photo/Jeff Watts)

The ultimate test of an election system is its ability to withstand intense public scrutiny during a very close election. Several close elections have taken place in recent years, and our election system has not always passed that test. We need a better election system.

1.4 URGENCY OF REFORM

Although the public continues to call for election reform, and several election bills have been introduced, the issue is low on the Congress's agenda at this time. Some congressional leaders believe that further reform should wait until HAVA is fully implemented. We believe that the need for additional electoral reform is abundantly clear, and our recommendations will bolster HAVA to further strengthen public confidence in the electoral process. If we wait until late 2006, we will lose the opportunity to put new reforms in place for the 2008 elections, and as a result, the next presidential election could be fraught with problems. Electoral reform may stay out of public view until the 2006 elections begin to approach, but by that time, it may be too late. We need Congress to press ahead with election reform now. Indeed, election reform is best accomplished when it is undertaken before the passions of a specific election cycle begin.

We are Republicans, Democrats, and Independents. But we have deliberately attempted to address electoral issues without asking the question as to whether a particular political party would benefit from a particular reform. We have done so because our country needs a clear unified voice calling for serious election reform. Congress has been reluctant to undertake reform, in part because members fear it could affect their chances of re-election and, when finally pressed by the public, Democrats and Republicans have addressed each reform by first asking whether it would help or harm each party's political prospects. This has proven to be not only a shortsighted but also a mistaken approach. Despite widespread belief that two recent reforms — the National Voter Registration Act of 1993 and the Bipartisan Campaign Finance Reform of 2002 — would advantage Democrats at the expense of Republicans, evidence suggests such beliefs were wrong. Having a fair electoral process in which all eligible citizens have an opportunity to participate freely is a goal that transcends any individual partisan interest. This assures the winning candidates the authority to legitimately assume office. For the losing candidate it assures that the decision can be accepted as the will of the voters.



League of Women Voters President Kay Maxwell at the April 18 hearing (American University Photo/Jeff Watts)

Our recommendations are aimed at several timeframes and audiences. Some require immediate action, and others can be considered later. We propose some for the federal government and some for the states. But we have offered all the recommendations based on our views as to how they can best help our country — not our political parties. Together, these reforms should catalyze a shift in the way that elections are administered. We hope they will not only restore American confidence in our elections, but also strengthen the respect from those in the world who look to our democracy as a model.



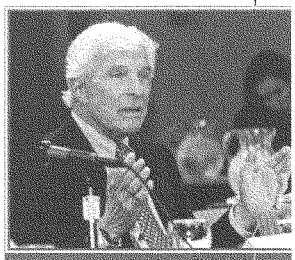
(AP Photo/Eric Francis)

2. Voter Registration and Identification

Effective voter registration and voter identification are bedrocks of a modern election system. By assuring uniformity to both voter registration and voter identification, and by having states play an active role in registering as many qualified citizens as possible, access to elections and ballot integrity will both be enhanced. These steps could help bring to an end the sterile debate between Democrats and Republicans on access versus integrity.

The most common problems on Election Day concern voter registration (see Table 1 on page 17). Voter registration lists often are riddled with inaccuracies because Americans are highly mobile, and local authorities, who have maintained most lists, are poorly positioned to add and delete names of voters who move within or between states. To comprehend the magnitude of this challenge, consider the following. During the last decade, on average, about 41.5 million Americans moved each year. Of those, about 31.2 million moved within the same state, and 8.9 million moved to a different state or abroad. Young Americans (aged 20 to 29), representing 14 percent of the U.S. population, moved to a different state at almost three times the rate of the rest of the population.[6] The process of registering voters should be made easier, and renewal due to a change of address should be made still easier.

In response to the challenge of building and maintaining better registration lists, HAVA requires states to establish statewide, computer-based registration lists that are interactive within each state by January 1, 2006. HAVA also requires provisional ballots for eligible voters who seek to vote within their jurisdiction but who are denied a ballot because their name is not found on the voter roll or because they are otherwise challenged by an election official as being ineligible to vote.



Commissioner Robert Brehm (American University Photo/Wilford Harewood)

Although few states have completed their new statewide voter databases, the limitations of the existing efforts are already clear. Several states have left the primary responsibility for voter lists in the hands of counties and municipalities. There is little if any effort to assure quality in statewide voter databases. The U.S. Election Assistance Commission (EAC) has not assessed the quality of statewide voter databases and is unlikely to do so in the future. Moreover, it has provided only vague guidance to states on how to organize their voter registration lists — on even the most basic question as to whether states or counties should be in charge.

In addition to statewide registration systems and provisional ballots, HAVA requires that states insist on voter identification only when a person has registered by mail for the first time in a federal election. This provision, like the others, was implemented very differently across the country, with some areas not even applying the minimum requirement. Since HAVA, an increasing number of states have insisted on stringent, though very different, ID requirements for all voters. This, in turn, has caused concern that such requirements could erect a new barrier to voting for people who do not have the requisite identification card. Georgia, for example, introduced a new law in July 2005 that requires all voters to show a government-issued photo ID at the polls.

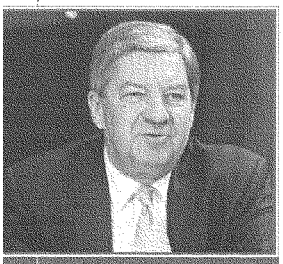
Although there are 159 counties, only 56 locations in the entire state issue such IDs, and citizens must either pay a fee for the ID or declare indigence.

While states will retain principal responsibility for the conduct of elections, greater uniformity in procedures for voter registration and identification is essential to guarantee the free exercise of the vote by all U.S. citizens. The EAC should facilitate greater uniformity in voter registration and identification procedures and should be empowered to do so by granting and withholding federal funds to the states. If Congress does not appropriate the funds, then we recommend that it amend the law to require uniformity of standards.

2.1 UNIFORMITY WITHIN STATES — TOP-DOWN REGISTRATION SYSTEMS

A complete, accurate, and current voter roll is essential to ensure that every eligible citizen who wants to vote can do so, that individuals who are ineligible cannot vote, and that citizens cannot vote more than once in the same election. A voter registration list must contain all eligible voters (including new registrants) and must contain correct information concerning the voter's identity and residence.

Incomplete or inaccurate registration lists lie at the root of most problems encountered in U.S. elections. When a voter list omits the names of citizens who believe they properly registered or contains incorrect or out-of-date information on registered voters, eligible citizens often are denied the right to vote. Invalid voter files, which contain ineligible, duplicate, fictional, or deceased voters, are an invitation to fraud.



Commissioner Benjamin Ginsberg (American University Photo/Jeff Watts)

One reason for flawed lists is decentralized management. Local authorities often fail to delete the names of voters who move from one jurisdiction to another, and thus the lists are often inflated. For this reason, the Carter-Ford National Commission on Federal Election Reform recommended the creation of statewide voter registration systems, and this recommendation was codified into law in HAVA.

HAVA requires each state to create a "single, uniform, official, centralized, interactive computerized statewide voter registration list defined, maintained, and administered at the state level." But states have not carried out this requirement in a consistent manner. Some are creating a "top-down" voter registration system, in which local election authorities supply information to a unified database maintained by the state. Others rely on a "bottom-up" system, whereby counties and municipalities retain their own registration lists and submit information to a state compilation of local databases at regular intervals. Top-down databases typically deliver information in real time — counties can see changes from other localities as these changes are made to the voter list. Bottom-up systems may continue

the problems that gave rise to flawed registration lists — i.e., counties retain control of the lists. Counties might not delete the names of voters who move or might not add the names of voters who register at motor vehicle bureaus or other state agencies under the National Voter Registration Act (NVRA or "Motor Voter"). Thus, the statewide lists might be different from the controlling county lists. Having two inconsistent voter lists is like a person with two watches who never knows what time it is. It is essential to have a single, accurate, current voter list.



Commissioners Ray Cobb, Jones and Raul Yzaguirre (American University Photo/Wilford Harwood)

As of June 2005, 38 states were establishing top-down voter registration systems. The remaining states were either (a) building bottom-up systems; or (b) creating systems with both top-down and bottom-up elements. Three states had not finalized plans.[7] The EAC, in its interpretation of the HAVA requirement on statewide voter databases, expressed a preference for top-down systems for voter registration but did not insist on it and did not rule out bottom-up systems.

In the judgment of our Commission, bottom-up sy ems are not capable of providing a complete, accurate, current, and valid voter registration list. They are ineffective in removing duplicate registrations of individuals who move from one county to another and in coordinating with databases of other state agencies. Even in the best of circumstances, with excellent cooperation and interaction between states and counties — an unlikely scenario with the bottom-up system — there will be a time lag in updating voter files in a bottom-up system. This time lag could be particularly harmful in the period approaching the deadline for voters to register.

Recommendation on Uniformity Within States

2.1.1 The Commission recommends that states be required to establish unified, top-down voter registration systems, whereby the state election office has clear authority to register voters and maintain the registration list. Counties and municipalities should assist the state with voter registration, rather than have the state assist the localities. Moreover, Congress should appropriate funds for disbursement by the U.S. Election Assistance Commission (EAC) to states to complete top-down voter registration systems.

2.2 INTEROPERABILITY AMONG STATES

Interoperable state voter databases are needed to facilitate updates in the registration of voters who move to another state and to eliminate duplicate registrations, which are a source of potential fraud. Approximately 9 million people move to another state or abroad each year, or about one in eight Americans between each presidential election. Such interoperability is possible because state voter databases that are centralized can be made to communicate with each other.

The limited information available on duplicate registrations indicates that a substantial number of Americans are registered to vote in two different states. According to news reports, Florida has more than 140,000 voters who apparently are registered in four other states (in Georgia, Ohio, New York, and North Carolina).[8] This includes almost 46,000 voters from New York City alone who are registered to vote in Florida as well. Voting records of the 2000 elections appear to indicate that more than 2,000 people voted in two states. Duplicate registrations are also seen elsewhere. As many as 60,000 voters are reportedly registered in both North Carolina and South Carolina.[9]

Current procedures for updating the registration of voters who move to another state are weak or nonexistent. When people register to vote, they are usually asked to provide their prior address, so that the jurisdiction where they lived can be notified to delete their names from the voter list. Such notification, however, often does not occur. When a voter moves from Virginia to Illinois, for example, a four-step process is required to update voter registration: (1) election authorities in Illinois must ask for prior address; (2) the voter must provide prior address; (3) Illinois election authorities must notify the correct election authorities in Virginia; and (4) Virginia election authorities must remove the voter from its list. Unless all four steps are taken, this voter will remain on the voter list in Virginia. In fact, states often fail to share data or notify each other of voters who move. As a result, a substantial number of Americans are registered to vote in more than one state.



From left to right, Ken Smukler, Michael Alvarez, Paula Hawthorn, and Robert Stein at the June 30 hearing (Rice University Photo/Jeff Fitlow)

Duplicate registrations have accumulated over the years not just because there are no systems to remove them other than the one described above, but also because people who own homes in two states can register to vote in both places. In fact, when 1,700 voters who were registered in both New York and Florida requested absentee ballots to be mailed to their home in the other state, no one ever bothered to investigate.[10]

Interoperability among state voter databases is needed to identify and remove duplicate registrations of citizens who are registered to vote in more than one state. To make the state voter databases interoperable, the Commission recommends the introduction of a uniform template, shared voter data, and a system to transfer voter data across states.[11]

The template will define a common set of voter data that all states will collect in their voter databases and will share with each other. This set of data will consist of each person's full legal name, date and place of birth, signature captured as a digital image, and Social Security number. The signature is needed to confirm the identity of voters who vote by mail.

Under HAVA, voter databases need a "unique identifier," which is a number used to distinguish each individual, particularly those with the same or similar names. Some states use the driver's license number as the unique identifier for voter registration. In other states, the unique identifier is the Social Security number. Efforts to match voter registrations in states that use different identifiers are complicated and may fail. Take, for example, the problem of figuring out whether Paul Smith in Michigan is the same person as Paul Smith in Kentucky. Since the unique identifier for voter registration is the driver's license number in Michigan but the Social Security number in Kentucky, an accurate match of the two registered Paul Smiths is not likely. Any match will need to rely on Paul Smith's date of birth to estimate, based on some level of probability, whether the Paul Smith in each state is the same person or not.

To make different state voter databases interoperable, therefore, they must use the same unique identifier, and this identifier must distinguish each American from every other voter in the country. The state voter databases will need to use a nationwide identifier. Since the same driver's license number might be used in different states, the Social Security number provides the most feasible option for a federal unique identifier.

While the use of Social Security numbers for voter registration raises concerns about privacy, these concerns can be adequately addressed by the measures the Commission recommends to ensure the security of voter databases. The Commission stresses the importance for states to allow only authorized election officials to use the Social Security numbers. States should not provide Social Security numbers in the voter lists they release to candidates, political parties, or anyone else. This should not be hard to do. Forty-nine states collect Social Security numbers for driver's licenses,[12] and they have protected the privacy of the Social Security numbers.

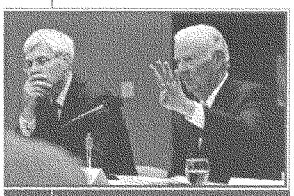


Commissioners Jack Nelson, Rene Nuñez, and Spencer Overton (American University Photo/Willard Hanewood)

Congress should direct that all states use the same unique identifier — i.e., the voter's Social Security number — and template, but a new system will also be needed to share data on voters among states. Such a system should maintain a uniform state voter list while allowing systematic updating of lists to take into account moves between states. The Commission proposes using a model similar to the one supervised by the U.S. Department of Transportation (DOT) to make sure that commercial drivers have only one license. The Commercial Driver's License Information System (CDLIS) shares data among states on commercial driver's licenses, using a "distributed database" — a collection of 51 databases (the 50 states and Washington, D.C.) that are linked to each other. When state officials want to check a particular driver's record, they go to the central site, which then connects them to the database of the state that issued a commercial license to that particular driver. Since all of the state databases are inter-connected, an update in one state database is immediately available to all other states. CDLIS is operated by the American Association of Motor Vehicle Administrators under the supervision of the U.S. Department of Transportation.

Similarly, our Commission recommends a "distributed database" that will connect all states' registration lists. The creation of a computerized system to transfer voter data between states is entirely feasible. This system could be managed either by the EAC or by an interstate compact or association of state officials under EAC supervision.

Implementation of the Commission's recommendation on cross-state interoperability of voter databases will require state election authorities to collect Social Security numbers and digital images of signatures for all registered voters. While many states use the driver's license number as their unique identifier, they can collect Social Security numbers from their state's department of motor vehicles (a Social Security number is required by 49 states to issue a driver's license).[13]



Commissioner Rutan Land and Commissioner Co-Chair James A. Baker III (American University Photo/Wilford Harewood)

We recommend that the EAC oversee the adoption of the template for voter data and for assisting states in the creation of a new system to share voter data among states, including for setting up a distributed database.

Congress should appropriate federal funds to complete top-down state voter databases, cover the costs of adding Social Security numbers and digital images of signatures to the databases, and create and maintain the federal distributed database system for sharing voter data among states. Congress should provide these funds to the EAC for distribution to states that adopt the uniform template for voter data and join the system for data sharing. Federal funds would be withheld from states that do not make their voter files interoperable with the voter databases of other states.

As states make their voter databases interoperable, they will retain full control over their registration lists. They will only need to add to their current databases the voter data required to complete the uniform template.

Two additional innovations might help to eliminate registration problems that voters have encountered. First, voters should have an opportunity during the registration process and before Election Day to review the registration online list to see whether their name is correctly inscribed and to check their proper precinct for voting.[14] Whenever an error is discovered, voters should notify the statewide registration office to correct it, and every statewide registration office should have procedures in place to correct such an error in a timely manner. Second, precincts should have an "electronic poll-book" that connects them to the statewide registration list and allows them to locate the correct polling site for each voter. For those precincts that are small, lack the resources for such an instrument, or do not have online access, precinct officials should telephone to a neighboring jurisdiction to obtain the correct information. Poll workers should also have a dedicated phone number to contact local election officials in case assistance is needed. This phone number should be different from the number provided to the public. Too often, poll workers cannot connect with election officials when assistance is needed because public phone lines are overwhelmed.

The entire system should permit state-of-the-art, computer-based registration lists that will be accurate and up-to-date for the entire nation.

Recommendations on Interoperability Among States

2.2.1 In order to assure that lists take account of citizens moving from one state to another, voter databases should be made interoperable between states. This would serve to eliminate duplicate registrations, which are a source of potential fraud.

2.2.2 In order to assist the states in creating voter databases that are interoperable across states, the EAC should introduce a template for shared data and a format for cross-state data transfers. This template should include a person's full legal name, date and place of birth, signature (captured as a digital image), and Social Security number.

2.2.3 With assistance and supervision by the EAC, a distributed database system should be established to make sure that the state lists remain current and accurate to take into account citizens moving between states. Congress should also pass a law mandating that states cooperate with this system to ensure that citizens do not vote in two states.

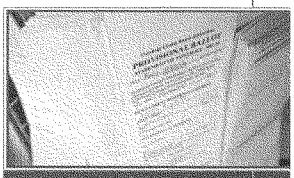
2.2.4 Congress should amend HAVA to mandate the interoperability of statewide registration lists. Federal funds should be appropriated for distribution by the EAC to states that make their voter databases interoperable, and the EAC should withhold federal funds from states that fail to do so. The law should also provide for enforcement of this requirement.

2.2.5 With proper safeguards for personal security, states should allow citizens to verify and correct the registration lists' information on themselves up to 30 days before the election. States should also provide "electronic poll-books" to allow precinct officials to identify the correct polling site for voters.

2.2.6 With interoperability, citizens should need to register only once in their lifetime and updating their registration will be facilitated when they move.

2.3 PROVISIONAL BALLOTS

Because of flaws in registration lists and other election administration procedures, HAVA mandated that any eligible voter who appears at the polls must be given a provisional ballot if his or her name does not appear on the voter registration list or an election official asserts that the individual is not eligible to vote. November 2, 2004, marked the first time that all states were supposed to offer provisional ballots in a general election. Out of 1.6 million provisional ballots cast, more than one million were counted.[15] The 1.6 million provisional ballots do not include an unknown number of voters who were encouraged by poll workers to go to other polling sites where they might be registered.



Provisional ballots cast during the 2004 presidential election (AP Photo/Tony Dejak)

Practices for offering and counting provisional ballots in the 2004 presidential election varied widely by state and by county. Around the country, the percentage of provisional ballots counted ranged from a national high in Alaska of 97 percent to a low of 6 percent in Delaware.[16]

This was due in part to whether a state accepted a provisional ballot cast outside of a voter's home precinct. In other situations, provisional ballots were counted without first having been verified as eligible ballots.

If the recommendations for strengthening the registration lists are approved, the need for provisional ballots will be reduced. In 2004, provisional ballots were needed half as often in states with unified databases as in states without.[17] Nonetheless, in the absence of the reforms recommended by this Commission, or in the period before they come fully into effect, provisional balloting will continue to be a crucial safety net. During the interim, in order to reduce the chances that elections are litigated, we need consistent procedures for handling provisional ballots and full training for poll workers who carry out these procedures.

Recommendations on Provisional Ballots

2.3.1 Voters should be informed of their right to cast a provisional ballot if their name does not appear on the voter roll, or if an election official asserts that the individual is not eligible to vote, but States should take additional and effective steps to inform voters as to the location of their precinct.

2.3.2 States, not counties or municipalities, should establish uniform procedures for the verification and counting of provisional ballots, and that procedure should be applied uniformly throughout the State. Many members of the Commission recommend that a provisional ballot cast in the incorrect precinct but in the correct jurisdiction should be counted.

2.3.3 Poll workers should be fully trained on the use of provisional ballots, and provisional ballots should be distinctly marked and segregated so they are not counted until the eligibility of the voter is determined.

2.4 COMMUNICATING REGISTRATION INFORMATION

The hotlines set up by nonprofit organizations to assist voters on Election Day received hundreds of thousands of calls (see Table 1 on page 17). Most of the callers had two simple questions: Am I registered to vote? And where do I go to vote? Answers to these questions, however, too often were difficult to obtain. Only nine state election Web sites were able to provide voters with their registration information or with the address of their polling site. Information was equally difficult to obtain from election offices by telephone. One Election Day hotline transferred callers to their county board of elections, but barely half of these calls were answered, and of the other half, few provided the information that was requested.[18]

Failure to provide voters with such basic information as their registration status and their polling site location raises a barrier to voting as significant as inconsistent procedures on provisional ballots or voter ID requirements. As states gain responsibility for voter registration, they will be well positioned to inform voters if they are listed in the voter files. The Web sites of local jurisdictions should allow voters to check whether they are registered and the location of their precinct. This precinct-locator feature should be added to state elections Web sites. In addition, information on how to register and where to vote should be disseminated in local media, on posted lists, and in other government offices, including welfare and social services agencies.

Since election officials may have difficulty responding to telephone calls on Election Day as they are conducting the election, states and local jurisdictions should encourage voters to inquire about their registration status and the location of their polling place considerably before Election Day.

TABLE 1 : Voter Calls to the MYVOTE1 Hotline on Election Day 2004

Topic of Question or Complaint on Election Day 2004	Percent of Total
Registration Issues/Poll Access	43.9%
Absentee Voting	24.2%
Coercion/Intimidation	4.9%
Mechanical	4.5%
Identification	2.5%
Provisional Ballots	1.9%
Ballot/Screen	1.3%
Other	16.8%
TOTAL	100.0%

NOTES: Totals are based upon an analysis of 55,000 phone calls to the MYVOTE1 hotline on November 2, 2004. Two major, nonpartisan hotlines and the U.S. Election Assistance Commission received a total of approximately 255,000 voter calls on Election Day 2004.

SOURCES: Testimony before the Commission on Federal Election Reform by Ken Smukler, President of Info Voter Technologies, on June 30, 2005; Testimony before the U.S. House of Representatives Administration Committee by the U.S. Election Assistance Commission, on February 9, 2005.

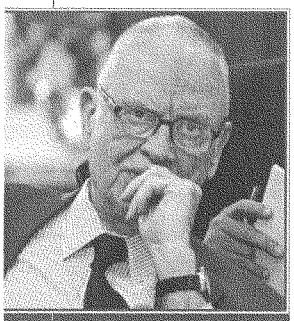
Recommendation on Communicating Registration Information

2.4.1 States and local jurisdictions should use Web sites, toll-free numbers, and other means to answer questions from citizens as to whether they are registered and, if so, what is the location of their precinct, and if they are not registered, how they can do so before the deadline.

2.5 VOTER IDENTIFICATION

A good registration list will ensure that citizens are only registered in one place, but election officials still need to make sure that the person arriving at a polling site is the same one that is named on the registration list. In the old days and in small towns where everyone knows each other, voters did not need to identify themselves. But in the United States, where 40 million people move each year, and in urban areas where some people do not even know the people living in their own apartment building let alone their precinct, some form of identification is needed.

There is no evidence of extensive fraud in U.S. elections or of multiple voting, but both occur, and it could affect the outcome of a close election.[19] The electoral system cannot inspire public confidence if no safeguards exist to deter or detect fraud or to confirm the identity of voters. Photo IDs currently are needed to board a plane, enter federal buildings, and cash a check. Voting is equally important.



Commissioner Lee Hamilton
(American University Photo/Willard Rosewood)

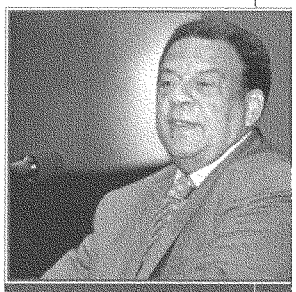
The voter identification requirements introduced by HAVA are modest. HAVA requires only first-time voters who register by mail to show an ID, and they can choose from a number of different types of identification. States are encouraged to allow an expansive list of acceptable IDs, including those without a photograph, such as utility bills or government checks. These requirements were not implemented in a uniform manner and, in some cases, not at all. After HAVA was enacted, efforts grew in the states to strengthen voter identification requirements. While 11 states required voter ID in 2001, 24 states now require voters to present an ID at the polls.[20] In addition, bills to introduce or strengthen voter ID requirements are under consideration in 12 other states.[21]

Our Commission is concerned that the different approaches to identification cards might prove to be a serious impediment to voting. There are two broad alternatives to this decentralized and unequal approach to identification cards. First, we could recommend eliminating any requirements for an ID because the evidence of multiple voting is thin, and ID requirements, as some have argued, are "a solution in search of a problem." Alternatively, we could recommend a single national voting identification card. We considered but rejected both alternatives.

We rejected the first option — eliminating any requirements — because we believe that citizens should identify themselves as the correct person on the registration list when they vote. While the Commission is divided on the magnitude of voter fraud — with some believing the problem is widespread and others believing that it is minor — there is no doubt that it occurs. The problem, however, is not the magnitude of the fraud. In close or disputed elections, and there are many, a small amount of fraud could make the margin of difference. And second, the perception of possible fraud contributes to low confidence in the system. A good ID system could deter, detect, or eliminate several potential avenues of fraud— such as multiple voting or voting by individuals using the identities of others or

those who are deceased — and thus it can enhance confidence. We view the other concerns about IDs — that they could disenfranchise eligible voters, have an adverse effect on minorities, or be used to monitor behavior — as serious and legitimate, and our proposal below aims to address each concern.

We rejected the second option of a national voting identification card because of the expense and our judgment that if these cards were only used for each election, voters would forget or lose them.



Former Atlanta Mayor Andrew Young addresses the Commission on August 30 at The Carter Center (American University Photo/Wilford Harwood)

We therefore propose an alternative path. Instead of creating a new card, the Commission recommends that states use "REAL ID" cards for voting purposes. The REAL ID Act, signed into law in May 2005, requires states to verify each individual's full legal name, date of birth, address, Social Security number, and U.S. citizenship before the individual is issued a driver's license or personal ID card. The REAL ID is a logical vehicle because the National Voter Registration Act established a connection between obtaining a driver's license and registering to vote. The REAL ID card adds two critical elements for voting — proof of citizenship and verification by using the full Social Security number.

The REAL ID Act does not require that the card indicates citizenship, but that would need to be done if the card is to be used for voting purposes. In addition, state bureaus of motor vehicles should automatically send the information to the state's bureau of elections. (With the National Voter Registration Act, state bureaus of motor vehicles ask drivers if they want to register to vote and send the information only if the answer is affirmative.)

Reliance on REAL ID, however, is not enough. Voters who do not drive,[12] including older citizens, should have the opportunity to register to vote and receive a voter ID. Where they will need identification for voting, IDs should be easily available and issued free of charge. States would make their own decision whether to use REAL ID for voting purposes or instead to rely on a template form of voter ID. Each state would also decide whether to require voters to present an ID at the polls, but our Commission recommends that states use the REAL ID and/or an EAC template for voting, which would be a REAL ID card without reference to a driver's license.

For the next two federal elections, until January 1, 2010, in states that require voters to present ID at the polls, voters who fail to do so should nonetheless be allowed to cast a provisional ballot, and their ballot would count if their signature is verified. After the REAL ID is phased in, i.e., after January 1, 2010, voters without a valid photo ID, meaning a REAL ID or an EAC-template ID, could cast a provisional ballot, but they would have to return personally to the appropriate election office within 48 hours with a valid photo ID for their vote to be counted.

To verify the identity of voters who cast absentee ballots, the voter's signature on the absentee ballot can be matched with a digitized version of the signature that the election administrator maintains. While such signature matches are usually done, they should be done consistently in all cases, so that election officials can verify the identity of every new registrant who casts an absentee ballot.

The introduction of voter ID requirements has raised concerns that they may present a barrier to voting, particularly by traditionally marginalized groups, such as the poor and minorities, some of whom lack a government-issued photo ID. They may also create obstacles for highly mobile groups of citizens. Part of these concerns are addressed by assuring that government-issued photo identification is available without expense to any citizen and, second, by government efforts to ensure that all voters are provided convenient opportunities to obtain a REAL ID or EAC-template ID card. As explained in Section 4.1, the Commission recommends that states play an affirmative role in reaching out with mobile offices to individuals who do not have a driver's license or other government-issued photo ID to help them register to vote and obtain an ID card.



Commissioners David Lebow, Betty Castor, and Tom Phillips (American University Photo/Willard Rarenscroft)

There are also longstanding concerns voiced by some Americans that national identification cards might be a step toward a police state. On that note, it is worth recalling that most advanced democracies have fraud-proof voting or national ID cards, and their democracies remain strong. Still, these concerns about the privacy and security of the card require additional steps to protect against potential abuse. We propose two approaches. First, new institutional and procedural safeguards should be established to assure people that their privacy, security, and identity will not be compromised by ID cards. The cards should not become instruments for monitoring behavior. Second, certain groups may see the ID cards as an obstacle to voting, so the government needs to take additional measures to register voters and provide ID cards.

The needed measures would consist of legal protections, strict procedures for managing voter data, and creation of ombudsman institutions. The legal protections would prohibit any commercial use of voter data and impose penalties for abuse. The data-management procedures would include background checks on all officials with access to voter data and requirements to notify individuals who are removed from the voter registration list. The establishment of ombudsman institutions at the state level would assist individuals to redress any cases of abuse. The ombudsman would be charged with assisting voters to overcome bureaucratic mistakes and hurdles and respond to citizen complaints about the misuse of data.

The Commission's recommended approach to voter ID may need to adapt to changes in national policy in the future. Since the attacks of September 11, 2001, concerns about homeland security have led to new policies on personal identification. Under a presidential directive, about 40 million Americans who work for or contract with the federal government are being issued ID cards with biometrics, and the REAL ID card may very well become the principal identification card in the country. Driven by security concerns, our country may already be headed toward a national identity card. In the event that a national identity card is introduced, our Commission recommends that it be used for voting purposes as well.

Recommendations on Voter Identification

2.5.1 To ensure that persons presenting themselves at the polling place are the ones on the registration list, the Commission recommends that states require voters to use the REAL ID card, which was mandated in a law signed by the President in May 2005. The card includes a person's full legal name, date of birth, a signature (captured as a digital image), a photograph, and the person's Social Security number. This card should be modestly adapted for voting purposes to indicate on the front or back whether the individual is a U.S. citizen. States should provide an EAC-template ID with a photo to non-drivers free of charge.

2.5.2 The right to vote is a vital component of U.S. citizenship, and all states should use their best efforts to obtain proof of citizenship before registering voters.

2.5.3 We recommend that until January 1, 2010, states allow voters without a valid photo ID card (Real or EAC-template ID) to vote, using a provisional ballot by signing an affidavit under penalty of perjury. The signature would then be matched with the digital image of the voter's signature on file in the voter registration database, and if the match is positive, the provisional ballot should be counted. Such a signature match would in effect be the same procedure used to verify the identity of voters who cast absentee ballots. After January 1, 2010, voters who do not have their valid photo ID could vote, but their ballot would only count if they returned to the appropriate election office within 48 hours with a valid photo ID.

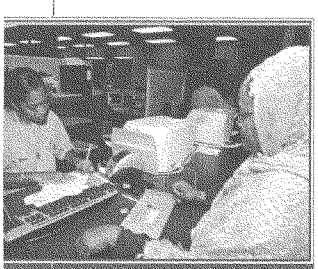
2.5.4 To address concerns about the abuse of ID cards, or the fear that it could be an obstacle to voting, states should establish legal protections to prohibit any commercial use of voter data and ombudsman institutions to respond expeditiously to any citizen complaints about the misuse of data or about mistaken purges of registration lists based on interstate matching or statewide updating.

2.5.5 In the event that Congress mandates a national identification card, it should include information related to voting and be connected to voter registration.

2.6 QUALITY IN VOTER REGISTRATION LISTS

Voter registration lists provide the basis for determining who is qualified to vote. Yet only a few states, notably Oregon and North Carolina, have assessed the quality of their lists, or have developed plans to do so. This is also true as states rush to complete statewide voter databases before the January 1, 2006, deadline. Moreover, the EAC does not assess the quality of voter files.

The little information available on the quality of voter files is not reassuring. The creation of statewide voter databases allows for the elimination of duplicate registrations within states, but attempts to match voter files with records of other state agencies are often ineffective. Death records, for example, sometimes are not provided to election officials for three or four months, and information on felons is usually incomplete.[23] Comparison with U.S. Census Bureau statistics also points to extensive "deadwood" on the voter registration lists. Some states have a large portion of inactive voters on their voter registration lists. One in four registered voters in Oregon is inactive, as is one in every three registered voters in California.[24] There also are numerous jurisdictions, such as Alaska, where the number of registered voters is greater than the number of voting-aged citizens.[25] These jurisdictions clearly have not updated their voter registration lists by removing the names of voters who have died or have moved away.



An election clerk in Detroit gives a voter an absentee ballot after verifying her registration status. (AP Photo/Carlos Osorio)

Voter registration lists are often inflated by the inclusion of citizens who have moved out of state but remain on the lists. Moreover, under the National Voter Registration Act, names are often added to the list, but counties and municipalities often do not delete the names of those who moved. Inflated voter lists are also caused by phony registrations and efforts to register individuals who are ineligible. Registration forms in the names of comic figures, for example, were submitted in Ohio in 2004. At the same time, inaccurate purges of voter lists have removed citizens who are eligible and are properly registered.

From what little is known, the quality of voter registration lists probably varies widely by state. Without quality assurance, however, cross-state transfers of voter data may suffer from the problem of "garbage in, garbage out." They may pass on inaccurate data from certain states to the rest of the country. The overall quality of a system to share voter data among states will only be a strong as the quality of the worst state voter database.

Each state needs to audit its voter registration files to determine the extent to which they are accurate (with correct and current information on individuals), complete (including all eligible voters), valid (excluding ineligible voters), and secure (with protections against unauthorized use). This can be done by matching voter files with records in other state agency databases in a regular and timely manner, contacting individuals when the matches are inconclusive, and conducting survey research to estimate the number of voters who believe they are registered but who are not in fact listed in the voter files. Other countries regularly conduct such audits.[26]

Effective audits assess not only the quality of voter files but also the procedures used to update, maintain, and verify data and to ensure security of voter databases. To assure continual quality of voter databases, effective procedures are needed to maintain up-to-date lists of eligible voters, verify the accuracy of those lists, and remove voters who have become ineligible. These should include procedures to delete those who have moved out of state and to effectively match voter files with records of driver's licenses, deaths, and felons. Given the controversial "purges" that have occurred, special care must be taken to update the lists in a fair and transparent manner. States should adopt uniform procedures and strong safeguards against incorrect removal of eligible voters. Every removal should be double-checked before it is executed, and a record should be kept of every action. The process of updating the lists should be continuous, and before each statewide election the voter rolls should be audited for accuracy.

In addition, states need to assure the privacy and security of voter files. There is no justification for states to release voter files for commercial purposes. However, components of voter files should remain public documents subject to public scrutiny. States must carefully balance the right to privacy of registered citizens with the need for transparency in elections when they decide what information on voter registration to make available to the public. Procedures are also needed to protect voter files against tampering or abuse. This might be done by setting up the voter database to make an automatic record of all changes to the voter files, including a record of who made the changes and when.

Recommendations on Quality in Voter Registration Lists

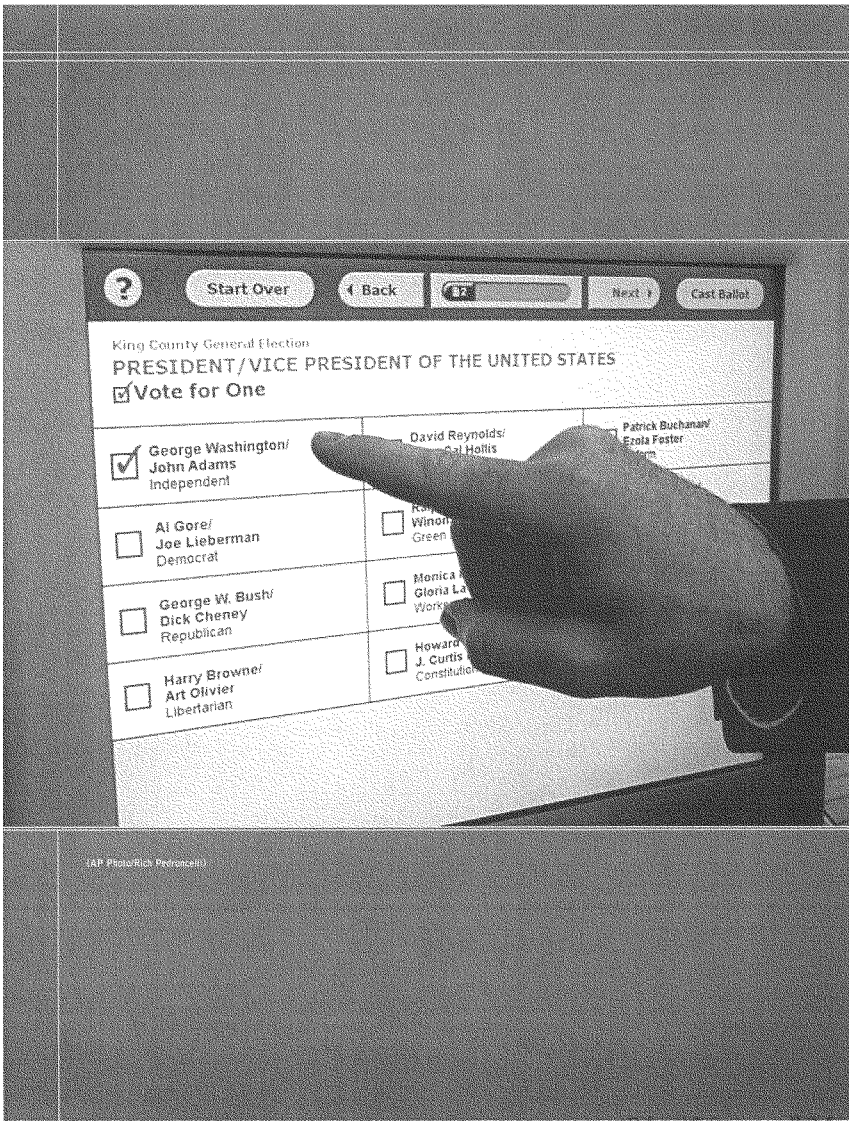
2.6.1 States need to effectively maintain and update their voter registration lists. The EAC should provide voluntary guidelines to the states for quality audits to test voter registration databases for accuracy (correct and up-to-date information on individuals), completeness (inclusion of all eligible voters), and security (protection against unauthorized access). When an eligible voter moves from one state to another, the state to which the voter is moving should be required to notify the state which the voter is leaving to eliminate that voter from its registration list.

2.6.2 All states should have procedures for maintaining accurate lists such as electronic matching of death records, drivers licenses, local tax rolls, and felon records.

2.6.3 Federal and state courts should provide state election offices with the lists of individuals who declare they are non-citizens when they are summoned for jury duty.

2.6.4 In a manner that is consistent with the National Voter Registration Act, states should make their best efforts to remove inactive voters from the voter registration lists. States should follow uniform and strict procedures for removal of names from voter registration lists and should adopt strong safeguards against incorrect removal of eligible voters. All removals of names from voter registration lists should be double-checked.

2.6.5 Local jurisdictions should track and document all changes to their computer databases, including the names of those who make the changes.


Start Over
Back
Next
Cast Ballot
King County General Election
PRESIDENT/VICE PRESIDENT OF THE UNITED STATES
Vote for One
George Washington/
John Adams
Independent
David Reynolds/
Patrick Buchanan/
Ezola Foster
Al Gore/
Joe Lieberman
Democrat
George W. Bush/
Dick Cheney
Republican
Harry Browne/
Art Olivier
Libertarian
(AP Photo/Rich Pedroncelli)

3. Voting Technology

The Help America Vote Act of 2002 authorized up to $650 million in federal funds to replace antiquated voting machines throughout the country. States are using these funds and their own resources to upgrade voting technology, generally to replace punch card and lever voting machines with new optical scan and electronic voting systems. As a result, voting technology is improving,[27] but new concerns related to electronic voting systems have arisen. These concerns need to be addressed, because it is vital to the electoral process that citizens have confidence that voting technologies are registering and tabulating votes accurately.

3.1 VOTING MACHINES

The purpose of voting technology is to record and tally all votes accurately and to provide sufficient evidence to assure all participants — especially the losing candidates and their supporters — that the election result accurately reflects the will of the voters.

Voting machines must be both accessible and transparent. As required by HAVA, the machines must be accessible to language minorities and citizens with disabilities, including the blind and visually impaired citizens, in a manner that allows for privacy and independence. Voting machines must also be transparent. They must allow for recounts and for audits, and thereby give voters confidence in the accuracy of the vote tallies.

Two current technology systems are optical scan and direct recording electronic (DRE) systems. Optical scan systems rely on preprinted paper ballots that are marked by the voter, like the ovals students fill in with a No. 2 pencil on a standardized exam, and then are run through an optical scan machine that determines and tallies the votes. Such systems provide transparency because the paper ballots can be recounted and audited by hand. Under HAVA, all aspects of the voting system, including the production of audit trail information, must be accessible to voters with disabilities.

DRE machines present voters with their choices on a computer screen, and voters choose by touching the screen or turning a dial. The vote is then recorded electronically, usually without ballot paper. DREs make up a growing share of voting equipment. Nearly 30 percent of voters live in jurisdictions that use DREs, compared to 17 percent in the 2000 election (see Table 2 on page 27).[28] DREs allow voters with disabilities to use audio prompts to cast ballots privately and independently, and they facilitate voting by non-English speakers by offering displays of the ballot in different languages. DREs also provide greater accuracy in recording votes, in part by preventing over-votes, whereby people mistakenly vote for more than one candidate, and by discouraging accidental under-votes by reminding voters when they overlooked one or more races.

The accessibility and accuracy of DREs, however, are offset by a lack of transparency, which has raised concerns about security and verifiability. In most of the DREs used in 2004, voters could not check that their ballot was recorded correctly. Some DREs had no capacity for an independent recount. And, of course, DREs are computers, and computers malfunction. A malfunction of DREs in Carteret County, North Carolina, in the November 2004 elections caused the loss of more than 4,400 votes. There was no backup record of the votes that were cast. As a result, Carteret County had no choice but to rerun

the election, after which it abandoned its DREs. Other jurisdictions have lost votes because election officials did not properly set up voting machines.[29]

To provide backup records of votes cast on DREs, HAVA requires that all voting machines produce a "permanent paper record with a manual audit capacity." This requirement is generally interpreted to mean that each machine must record individual ballot images, so that they can be printed out and examined in the event of a disputed result or of a recount. This will make DREs somewhat more transparent, but it is still insufficient to fully restore confidence.

One way to instill greater confidence that DREs are properly recording votes is to require a paper record of the ballot that the voter can verify before the ballot is cast. Such a paper record, known as a voter-verifiable paper audit trail (VVPAT), allows the voter to check that his or her vote was recorded as it was intended.

Because voter-verifiable paper audit trails can permit recounts, audits, and a backup in case of a malfunction, there is a growing demand for such paper trails. As of early August 2005, 25 states required voter-verifiable paper ballots, and another 14 states had proposed legislation with such a requirement.[30]

Since very few of the DREs in use today are equipped to print voter-verifiable paper audit trails, certain bills before Congress would require election authorities to "retrofit" DREs with such printers. In 2004, DREs with voter-verifiable paper audit trails were used only in Nevada. They appear to have worked well.[31] When Nevadans went to the polls and made their selection, a paper record of their vote was printed behind a glass cover on a paper roll, like the roll of paper in a cash register. Voters were able to view the paper record and thereby check that their vote was recorded accurately before they cast their ballot. The paper record was saved in the machine and thus was available for later use in recounts or audits. After the 2004 elections, Nevada election officials conducted an internal audit, which confirmed the accuracy of the votes recorded by the DREs. While less than one in three Nevada voters reportedly looked at the paper record of their ballot, these voters had the opportunity to confirm their vote, and the paper allowed a chance to verify the computer tallies after the election.

While HAVA already requires that all precincts be equipped with at least one piece of voting equipment that is fully accessible to voters with disabilities for use in federal elections by January 1, 2006, must be accessible to voters with disabilities, the Commission believes that transparency in voting machines should also be assured in time for the 2008 presidential election. With regard to current technology, states will need to use either DREs with a voter-verifiable paper audit trail and an audio prompt for blind voters or optical scan voting systems with at least one computer-assisted marking device for voters with disabilities to mark their ballot. To ensure implementation of this requirement, Congress will need to appropriate sufficient funds to cover the costs of either retrofitting DREs with voter-verifiable paper audit trails or purchasing a computer-assisted marking device for each polling place that uses optical scan voting systems.

Concerns have been raised that the printers could malfunction just as computers do. Of course, the previous ballot papers will be available, and the operators will know when the printers fail. Still, precincts should have backup printers for that contingency. A second concern is that the length of the ballot in some areas — such as California, which frequently

has referenda — would require paper trails that would be several feet long. In the case of non-federal races, state law would determine whether the non-federal portion of the ballot would similarly be required to provide a voter-verified paper audit trail. That is not a perfect solution, but it is still better than having no paper backup at all.

The standards for voting systems, set by the EAC, should assure both accessibility and transparency in all voting machines. Because these standards usually guide the decisions of voting machine manufacturers, the manufacturers should be encouraged to build machines in the future that are both accessible and transparent and are fully capable of meeting the needs of Americans with disabilities, of allowing voters to verify their ballots, and of providing for independent audits of election results.

TABLE 2: Types of Voting Equipment Used in Recent Presidential Elections

Type of Voting Equipment	Registered Voters in 2000 (by percentage)	Registered Voters in 2004 (by percentage)
Punch Card	27.9%	12.4%
Lever	17.0%	14.0%
Paper Ballots	1.3%	0.7%
DataVote	2.8%	1.3%
Optical Scan	29.5%	34.9%
Electronic	12.6%	29.4%
Mixed	8.9%	7.4%
TOTAL	100.0%	100.0%

SOURCE Election Data Services, Voting Equipment Summary by Type, 2004. Election Data Services, New Study Shows 50 Million Voters Will Use Electronic Voting Systems, 32 with Punch Cards in 2004.

Recommendations on Voting Machines

3.1.1 Congress should pass a law requiring that all voting machines be equipped with a voter-verifiable paper audit trail and, consistent with HAVA, be fully accessible to voters with disabilities. This is especially important for direct recording electronic (DRE) machines for four reasons: (a) to increase citizens' confidence that their vote will be counted accurately, (b) to allow for a recount, (c) to provide a backup in cases of loss of votes due to computer malfunction, and (d) to test — through a random selection of machines — whether the paper result is the same as the electronic result. Federal funds should be appropriated to the EAC to transfer to the states to implement this law. While paper trails and ballots currently provide the only means to meet the Commission's recommended standards for transparency, new technologies may do so more effectively in the future. The Commission therefore urges research and development of new technologies to enhance transparency, security, and auditability of voting systems.

3.1.2 States should adopt unambiguous procedures to reconcile any disparity between the electronic ballot tally and the paper ballot tally. The Commission strongly recommends that states determine well in advance of elections which will be the ballot of record.

3.2 AUDITS

While voter-verifiable paper ballots will contribute to strengthening public confidence in DREs, regular audits of voting machines are also needed to double-check the accuracy of the machines' vote tallies. Such audits were required by law in 10 states as of mid-August 2005.[52] To carry out such audits, election officials would randomly select a sample of voting machines and compare the vote total recorded by the machines with the vote total on the paper ballots. The audits would test the reliability of voting machines and identify problems, often before a close or disputed election takes place. This, in turn, would encourage both suppliers and election officials to effectively maintain voting machines.

Some concern has been expressed about the possibility of manipulation of paper audit trails.[53] If DREs can be manipulated to alter the vote tallies, the same can be done with paper audit trails. Such manipulation can be detected and deterred by regular audits of voting machines. Regular audits should be done of all voting machines, including DREs and optical scan systems.

Recommendation on Audits

3.2.1 State and local election authorities should publicly test all types of voting machines before, during, and after Election Day and allow public observation of zero machine counts at the start of Election Day and the machine certification process.

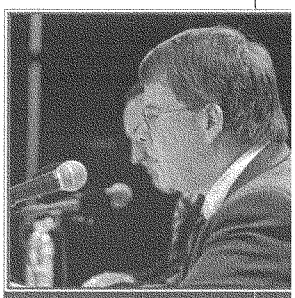
3.3 SECURITY FOR VOTING SYSTEMS

DREs run on software that can be compromised. DRE software may get attacked or hacked by outsiders, perhaps through the Internet. As experience in computer security shows, it is often difficult to defend against such attacks. Hackers often are creative and determined, and voting systems provide a tempting target. However, while some DREs send their results to election headquarters over the Internet, they are not connected to the Internet during voting.

The greater threat to most systems comes not from external hackers, but from insiders who have direct access to the machines. Software can be modified maliciously before being installed into individual voting machines. There is no reason to trust insiders in the election industry any more than in other industries, such as gambling, where sophisticated insider fraud has occurred despite extraordinary measures to prevent it. Software can also be programmed incorrectly. This poses a likely threat when local programmers who lack the necessary skills nonetheless modify the ballot for local offices, and many might not have the sophistication required for the new machines.

In addition to the output of DREs, which can be verified through a paper audit trail, the inside process of programming DREs should be open to scrutiny by candidates, their supporters, independent experts, and other interested citizens, so that problems can be detected, deterred, or corrected, and so that the public will have confidence in the machines.

At the same time, manufacturers of voting machines have legitimate reason to keep their voting machine software and its source code proprietary. The public interest in transparency and the proprietary interests of manufacturers can be reconciled by placing the source code in escrow with the National Institute of Standards and Technology (NIST), and by making the source code available for inspection on a restricted basis to qualified individuals. NIST might make the source code available to recognized computer security experts at accredited universities and to experts acting on behalf of candidates or political parties under a nondisclosure agreement, which would bar them from making information about the source code public, though they could disclose security flaws or vulnerabilities in the voting system software.



Stanford University Professor David Dill at the April 18 hearing (American University Photosoft Watch)

Doubt has been raised that some manufacturers of voting machines provide enough security in their systems to reduce the risk of being hacked. Such concerns were highlighted after a group of computer security experts examined a voting system source code that was accidentally left on the Internet.[14] Independent inspection of source codes would strengthen the security of voting systems software by encouraging manufacturers to improve voting system security. Expert reviews may also detect software design flaws or vulnerabilities. This, in turn, could bolster public confidence in the reliability of DREs to accurately record and tally the vote in elections.

In addition to the source codes, the software and the voting machines themselves are potentially vulnerable to manipulation. Security for voting systems should guard against attempts to tamper with software or individual voting machines. When voting machines are tested for certification, a digital fingerprint, also known as a "hash," of their software is often sent to NIST. Following the delivery of new voting machines, a local jurisdiction can compare the software on these machines to the digital fingerprint at NIST. This comparison either will identify changes made to the software before delivery or, if the software is unaltered, will confirm that the software on the individual machines meets the certified standards.

Once voting machines arrive at the local jurisdiction, election officials must take precautions to ensure security by restricting access to authorized personnel and by documenting access to the machines.

The process of testing and certifying voting machines is designed mainly to ensure their reliability. Testing and certification is conducted under EAC supervision, although some states require additional testing and certification. The state testing can make the process more rigorous, particularly when voting machines are field tested. When California conducted a mock election with new voting machines in July 2005, it found unacceptable rates of malfunctions that were not apparent in lab tests.[15]

No matter how secure voting machines are or how carefully they are used, they are liable to malfunction. To avoid a situation where a machine malfunction will cause a major disruption, local jurisdictions need to prepare for Election Day with a backup plan, including how the vendor will respond to a machine malfunction and what alternatives, including paper ballots, should be made available.

Recommendations on Security for Voting Systems

3.3.1 The Independent Testing Authorities, under EAC supervision, should have responsibility for certifying the security of the source codes to protect against accidental or deliberate manipulation of vote results. In addition, a copy of the source codes should be put in escrow for future review by qualified experts. Manufacturers who are unwilling to submit their source codes for EAC-supervised testing and for review by independent experts should be prohibited from selling their voting machines.

3.3.2 States and local jurisdictions should verify upon delivery of a voting machine that the system matches the system that was certified.

3.3.3 Local jurisdictions should restrict access to voting equipment and document all access, as well as all changes to computer hardware or software.

3.3.4 Local jurisdictions should have backup plans in case of equipment failure on Election Day.

3.4 INTERNET VOTING

The Internet has become such a pervasive influence on modern life that it is natural for the public and election officials to begin considering ways to use it to facilitate voting. The first binding Internet election for political office took place in 2000, when the Arizona Democratic Party used it during its primary. In 2004, the Michigan Democratic Party allowed voting by Internet during its caucuses. Meanwhile, Missouri announced that any member of the U.S. military serving in combat areas overseas could complete an absentee ballot for the general election and email a scanned copy to the Department of Defense, which then would forward it to the appropriate local election offices.

Despite these much-publicized trials, serious concerns have been raised about the push for a "digital democracy." In 2004, the Department of Defense cancelled its $22 million Secure Electronic and Voting Registration Experiment (SERVE) program designed to offer Internet voting during the presidential election to members of the U.S. military and other overseas citizens. The cancellation came after a group of top computer scientists who reviewed the system reported that without improved security, Internet voting is highly susceptible to fraud.

First, there are the issues of privacy and authentication. When using the Internet, one cannot assure voters that their ballot will remain secret. Second, the current system is not fully secure. Although data sent via the Internet can be encrypted and then decoded by local election administrators, hackers can compromise the system. This was the conclusion of the computer scientists who reviewed the SERVE program for the Pentagon. Due to security threats, some state and local election offices do not allow vote totals to be transmitted via the Internet. Third, no government or industry standards specifically apply to Internet voting technology. The EAC may begin developing such standards, but that work has not begun. Finally, Internet voting from homes and offices may not provide the same level of privacy as the voting booth.

To date, the most comprehensive study of Internet voting is contained in a 2001 report sponsored by the National Science Foundation.[36] This report urges further research and experimentation to deal with the problems posed by this form of voting. Its authors suggest that it will take at least a decade to examine the various security and authentication issues. Our Commission agrees that such experimentation is necessary, and that the time for Internet voting has not yet arrived.



Harris County (TX) election official Elsa Garcia, far right, demonstrates an electronic voting machine for Commissioners (L-r) Sissie Mobram, Tom Ducote, and Betty Castor (Rice University Photo/Jeff Fitlow)



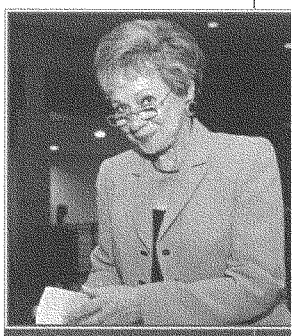
(AP Photo/Julia Cumes)

4. Expanding Access to Elections

The Commission believes that the vitality of America's democracy depends on the active participation of our citizens. Yet, even in the presidential election in 2004, when voter interest was higher than normal, more than one in three eligible voters did not participate. We need to do more to increase voter participation, and we have considered numerous methods. None of them will solve the problem, but we encourage states to experiment with alternatives to raise the level of voter participation.

Recent elections have seen a substantial increase in early voting and in voting by mail. While only 8 percent of ballots were cast before Election Day in 1994, by 2004 the percentage of ballots cast before Election Day had risen to 22 percent. This increase in early and convenience voting has had little impact on voter turnout, because citizens who vote early or vote by mail tend to vote anyway.[17] Early and convenience voting are popular, but there is little evidence that they will significantly expand participation in elections.[18]

There are other measures that can be taken to expand participation, particularly for military and overseas voters and for citizens with disabilities. There is also much to do with regard to civic and voter education that could have a long-term and lasting effect, particularly on young people. However, we first need to reach out to all eligible voters and remove any impediments to their participation created by the registration process or by identification requirements.



Commissioner Rita DiMartino (American University Photo/Willard Harewood)

All citizens, including citizens with disabilities, need to have access to polling places. Polling places should be located in public buildings and other semipublic venues such as churches and community centers that comply with the Americans with Disability Act (ADA). Additionally, polling places should be located and protected so that voters can participate free of intimidation and harassment. Polling places should not be located in a candidate's headquarters or in homes or business establishments that are not appropriately accessible to voters with disabilities.

4.1 ASSURED ACCESS TO ELECTIONS

The Commission's proposals for a new electoral system contain elements to assure the quality of the list and the integrity of the ballot. But to move beyond the debate between integrity and access, specific and important steps need to be taken to assure and improve access to voting.

States have a responsibility to make voter registration accessible by taking the initiative to reach out to citizens who are not registered, for instance by implementing provisions of the National Voter Registration Act that allow voter registration at social-service agencies or by conducting voter registration and REAL ID card drives with mobile offices. Michigan, for



A woman in St. Louis goes door-to-door soliciting new voter registrants for the 2004 election (AP Photo/Ron Edmonds).

example, uses a mobile office to provide a range of services, including driver's licenses and voter registration. This model should be extended to all the states.

Political party and nonpartisan voter registration drives generally contribute to the electoral process by generating interest in upcoming elections and expanding participation. However, they are occasionally abused. There were reports in 2004 that some party activists failed to deliver voter registration forms of citizens who expressed a preference for the opposing party. During the U.S. House Administration Committee hearings in Ohio, election officials reported being deluged with voter registration forms at the last minute before the registration deadline, making it difficult to process these registrations in a timely manner. Many of the registration forms delivered in October to election officials were actually collected in the spring.

Each state should therefore oversee political party and nonpartisan voter registration drives to ensure that they operate effectively, that registration forms are delivered promptly to election officials, that all completed registration forms are delivered to the election officials, and that none are "culled" and omitted according to the registrant's partisan affiliation. Measures should also be adopted to track and hold accountable those who are engaged in submitting fraudulent voter registrations. Such oversight might consist of training activists who conduct voter registration drives and tracking voter registration forms to make sure they are all accounted for. The tracking of voter registration forms will require better cooperation between the federal and state governments, perhaps through the EAC, as the federal government puts some registration forms online. In addition, states should apply a criminal penalty to any activist who deliberately fails to deliver a completed voter registration form.

Recommendations on Assured Access to Elections

4.1.1 States should undertake their best efforts to make voter registration and ID accessible and available to all eligible citizens, including Americans with disabilities. States should also remove all unfair impediments to voter registration by citizens who are eligible to vote.

4.1.2 States should improve procedures for voter registration efforts that are not conducted by election officials, such as requiring state or local registration and training of any "voter registration drives."

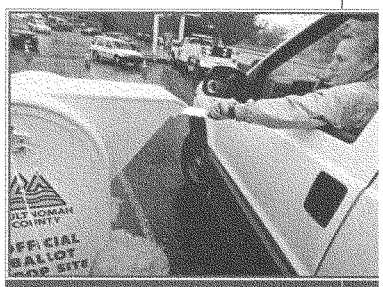
4.1.3 Because there have been reports that some people allegedly did not deliver registration forms of those who expressed a preference for another party, states need to take special precautions to assure that all voter registration forms are fully accounted for. A unique number should be printed on the registration form and also on a detachable receipt so that the voter and the state election office can track the status of the form.[19] In addition, voter registration forms should be returned within 14 days after they are signed.

4.2 VOTE BY MAIL

A growing number of Americans vote by mail. Oregon moved entirely to a vote-by-mail system in 1998, and the practice of casting ballots by mail has continued to expand nationwide as voters and election officials seek alternatives to the traditional system of voting at polling stations. The state legislatures of California and of Washington state have considered legislation to expand the use of vote by mail, and in 24 states no excuse is required to vote absentee.

The impact of vote by mail is mixed. Proponents argue that vote by mail facilitates participation among groups that experience low voter turnout, such as elderly Americans and Native Americans.

While vote by mail appears to increase turnout for local elections, there is no evidence that it significantly expands participation in federal elections.[40] Moreover, it raises concerns about privacy, as citizens voting at home may come under pressure to vote for certain candidates, and it increases the risk of fraud. Oregon appears to have avoided significant fraud in its vote-by-mail elections by introducing safeguards to protect ballot integrity, including signature verification. Vote by mail is, however, likely to increase the risks of fraud and of contested elections in other states, where the population is more mobile, where there is some history of troubled elections, or where the safeguards for ballot integrity are weaker.



An Oregon voter drops off his mail ballot (AP Photo/Rick Bowmer)

The case of King County, Washington, is instructive. In the 2004 gubernatorial elections, when two in three ballots there were cast by mail, authorities lacked an effective system to track the number of ballots sent or returned. As a result, King County election officials were unable to account for all absentee ballots. Moreover, a number of provisional ballots were accepted without signature verification.[41] The failures to account for all absentee ballots and to verify signatures on provisional ballots became issues in the protracted litigation that followed Washington state's 2004 gubernatorial election.

Vote by mail is popular but not a panacea for declining participation. While there is little evidence of fraud in Oregon, where the entire state votes by mail, absentee balloting in other states has been one of the major sources of fraud. Even in Oregon, better precautions are needed to ensure that the return of ballots is not intercepted.

The evidence on "early" voting is similar to that of vote by mail. People like it, but it does not appear to increase voter participation, and there are some drawbacks. It allows a significant portion of voters to cast their ballot before they have all of the information that will become available to the rest of the electorate. Crucial information about candidates may emerge in the final weeks or even days of an election campaign. Early and convenience voting also detracts from the collective expression of citizenship that takes place on Election

Day. Moreover, the cost of administering elections and of running campaigns tends to increase when early and mail-in voting is conducted in addition to balloting on Election Day. Early voting should commence no earlier than 15 days prior to the election, so that all voters will cast their ballots on the basis of largely comparable information about the candidates and the issues.

Recommendation on Vote by Mail

4.2.1 The Commission encourages further research on the pros and cons of vote by mail and of early voting.

4.3 VOTE CENTERS

Another alternative to voting at polling stations is the innovation of "vote centers," pioneered by Larimer County, Colorado. Vote centers are larger in size than precincts but fewer in number. They are dispersed throughout the jurisdiction, but close to heavy traffic routes, larger residential areas, and major employers. These vote centers allow citizens to vote anywhere in the county rather than just at a designated precinct. Because these vote centers employ economies of scale, fewer poll workers are required, and they tend to be more professional. Also, the vote centers are reported to use more sophisticated technology that is more accessible to voters with disabilities. Vote centers eliminate the incidence of out-of-precinct provisional ballots, but they need to have a unified voter database that can communicate with all of the other centers in the county to ensure that eligible citizens vote only once.

While vote centers appear to have operated effectively in Larimer County, further research is needed to determine if the costs of establishing vote centers are offset by the savings of eliminating traditional polling sites. Moreover, because vote centers replace traditional voting at precincts, which are generally closer to a voter's home, it is not clear that citizens actually view them as more convenient.

Recommendations on Vote Centers

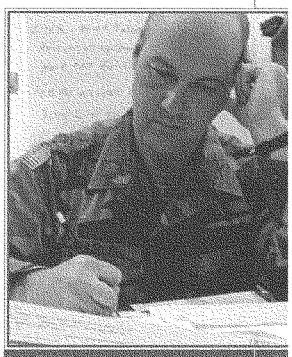
4.3.1 States should modify current election law to allow experimentation with voting centers. More research, however, is needed to assess whether voting centers expand voter participation and are cost effective.

4.3.2 Voting centers need a higher quality, computer-based registration list to assure that citizens can vote at any center without being able to vote more than once.

4.4 MILITARY AND OVERSEAS VOTING

Military and overseas voting present substantial logistical challenges, yet we cannot overstate the imperative of facilitating participation in elections by military and overseas voters, particularly by service men and women who put their lives on the line for their country. The Commission calls on every state, with federal government assistance, to make every effort to provide all military and overseas voters with ample opportunity to vote in federal elections.

More than six million eligible voters serve in the Armed Forces or live overseas. These voters include 2.7 million military and their dependents and 3.4 million diplomats, Peace Corps volunteers, and other civilian government and other citizens overseas.[42]



A U.S. Army officer stationed in Ghana fills in his 2004 voting forms (AP Photo/Ranel Ennis)

Voter turnout among members of the armed forces is high. So is the level of frustration they experience when their votes cannot be counted. This happens largely because of the time required by the three-step process of applying for an absentee ballot, receiving one, and then returning a completed ballot. The process is complicated by the differences among states and among localities in the registration deadline, ballot format, and requirements for ballot return, and it is exacerbated because of the mobility of service men and women during a time of conflict. Since September 11, 2001, more than 500,000 National Guard and Reserve personnel have been mobilized, and many were relocated before they received their absentee ballots.

Congress passed the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) in 1986 to help eligible members of the armed services and their families, and other citizens overseas, to vote. UOCAVA required each state to have a single office to provide information on voter registration and absentee ballot procedures for military voters. The Help America Vote Act of 2002 (HAVA) recommended — but did not require — that this state office should coordinate voting by military personnel by receiving absentee ballot applications and collecting voted ballots. The introduction of statewide voter registration databases under HAVA provides an opportunity to put this recommendation into practice. But aside from Alaska, which already had a single state office, no state has centralized the processing of absentee ballots. This is another example as to why recommending, rather than requiring, a course of action is insufficient.

The Commission recommends that when registering members of the armed forces and other overseas voters, states should inquire whether to send an absentee ballot to them automatically, thus saving a step in the process.

In the 2004 presidential election, approximately one in four military voters did not vote for a variety of reasons: The absentee ballots were not returned or arrived too late; they were rejected for procedural deficiencies, such as a signature not properly witnessed on the back of the return envelope; blank ballots were returned as undeliverable; or Federal Post Card Applications were rejected.[43]

The U.S. Department of Defense's Federal Voting Assistance Program, which assists military and overseas voters, tried to reduce the time lag for absentee voting by launching an electronic voting experiment. However, this experiment was ended because of fundamental security problems (see above on "Internet voting").[44] In the meantime, the Federal Voting Assistance Program encouraged states to send blank ballots out electronically and to accept voted ballots by fax. There now are 32 states that permit fax delivery of a blank ballot to military voters and 25 states that allow military voters to return their voted ballot by fax. In addition, some jurisdictions allow the delivery of blank ballots by email.[45] The return of voted ballots by fax or email, however, is a violation of the key principle of a secret ballot, and it is vulnerable to abuse or fraud.

Although the Uniformed and Overseas Citizens Absentee Voting Act applies to both military and nonmilitary voters overseas, procedures to facilitate overseas voting serve military voters better than civilians. To provide civilian overseas voters with equal opportunities to participate in federal elections, new approaches are needed at both the federal and state levels.

Recommendations on Military and Overseas Voting

4.4.1 The law calling for state offices to process absentee ballots for military and overseas government and civilian voters should be implemented fully, and these offices should be under the supervision of the state election offices.

4.4.2 New approaches should be adopted at the federal and state levels to facilitate voting by civilian voters overseas.

4.4.3 U.S. Department of Defense (DOD) should supply to all military posted outside the United States a Federal Postcard Application for voter registration and a Federal Write-in Absentee Ballot for calendar years in which there are federal elections. With adequate security protections, it would be preferable for the application forms for absentee ballots to be filed by Internet.

4.4.4 The states, in coordination with the U.S. Department of Defense's Federal Voting Assistance Program, should develop a system to expedite the delivery of ballots to military and overseas civilian voters by fax, email, or overnight delivery service, but voted ballots should be returned by regular mail, and by overnight mail whenever possible. The Defense Department should give higher priority to using military aircraft returning from bases overseas to carry ballots. Voted ballots should not be returned by email or by fax as this violates the secrecy of the ballot and is vulnerable to fraud.

4.4.5 All ballots subject to the Uniform and Overseas Civilians Absentee Voting Act must be mailed out at least 45 days before the election (if request is received by then) or within two days of receipt after that. If the ballot is not yet set, due to litigation, a late vacancy, etc., a temporary ballot listing all settled offices and ballot issues must be mailed.

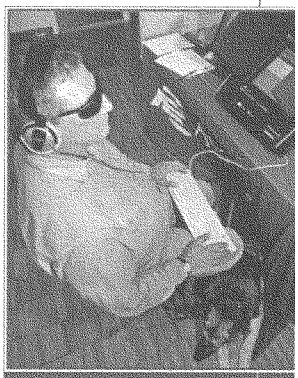
4.4.6 States should count the ballots of military and overseas voters up to 10 days after an election if the ballots are postmarked by Election Day.

4.4.7 As the technology advances and the costs decline, tracking systems should be added to absentee ballots so that military and overseas voters may verify the delivery of their voted absentee ballots.

4.4.8 The Federal Voting Assistance Program should receive a copy of the report that states are required under HAVA to provide the EAC on the number of absentee ballots sent to and received from military and overseas voters.

4.5 ACCESS FOR VOTERS WITH DISABILITIES

There are almost 30 million voting-aged Americans with some kind of disability—about 15 percent of the population (see Table 3 on page 40). Less than half of them vote. There are federal laws to facilitate voting and registration by eligible Americans with disabilities, but these laws have not been implemented with any vigor. As a result, voters with disabilities still face serious barriers to voting.[46] Congress passed the Voting Accessibility for the Elderly and Handicapped Act in 1984 and the Americans with Disabilities Act of 1990, which required local authorities to make polling places physically accessible to people with disabilities for federal elections. Yet a Government Accountability Office survey of the nation's polling places in 2000 found that 84 percent of polling places were not accessible on Election Day. By 2004, accessibility for voters with disabilities had improved only marginally. Missouri, for example, surveyed every polling place in the state and found that 71 percent were not accessible. Most other states have not even conducted surveys.[47]



A voter tries out a disability-accessible voting machine (AP Photo/Mike Peters)

There is similarly weak implementation of laws designed to facilitate voter registration by citizens with disabilities. Section 7 of the National Voter Registration Act (NVRA) requires state-funded agencies which provide services to citizens with disabilities to offer the opportunity to register citizens to vote. Implementation of this requirement, according to advocates for voters with disabilities, is rare or poor.[48]

HAVA provided additional support to Section 7 of NVRA by including social-service agencies as places to register voters, but only one state, Kentucky, has complied with Section 7, according to advocates for voters with disabilities. Moreover, at the current time, there is not a single case where the new statewide voter databases comply with Section 7.[49] Thus, 12 years after the National Voter Registration Act was passed, voters with disabilities still cannot apply for voter registration at all social service offices.

TABLE 3: Estimates of U.S. Voting Population with Disabilities by Type

Disability Type	Population Age 16 and Older (in millions)	Percent of Total Voting Age Population
Sensory, Physical, Mental or Self-Care Disability	29.5	15%
Self-Care Disability	6.4	3%
Physical Disability	12.5	6%
Mental Disability	4.0	2%
Sensory Disability	3.9	2%
Sensory and Physical Disability	2.5	1%
Sensory, Physical, and Mental Disability	2.0	1%
Total Voting Age Population in the U.S. (18 and older)	203.0	100%

NOTES: Respondents were able to report more than one type of disability.

SOURCES: U.S. Census Bureau, Selected Types of Disability for the Civilian Noninstitutionalized Population 5 Years and Over by Age: 2000; U.S. Census Bureau, Voting and Registration in the Election of November 2000.

Recommendations on Access for Voters With Disabilities

4.5.1 To improve accessibility of polling places for voters with disabilities, the U.S. Department of Justice should improve its enforcement of the Americans with Disabilities Act and the accessibility requirements set by the Help America Vote Act.

4.5.2 States should make their voter registration databases interoperable with social-service agency databases and facilitate voter registration at social-service offices by citizens with disabilities.

4.5.3 States and local jurisdictions should allow voters with disabilities to request an absentee ballot when they register and to receive an absentee ballot automatically for every subsequent election. Local election officials should determine which voters with disabilities would qualify.

4.6 RE-ENFRANCHISEMENT OF EX-FELONS

Only Maine and Vermont allow incarcerated citizens to vote. In all other states, citizens who are convicted of a felony lose their right to vote, either temporarily or permanently. An estimated 4.65 million Americans have currently or permanently lost their right to vote as a result of a felony conviction. Most states reinstate that right upon completion of the full sentence, including of parole, but three states — Florida, Kentucky, and Virginia — permanently ban all ex-felons from voting, and another 10 states have a permanent ban on

voting by certain categories of ex-felons.[50] These laws have a disproportionate impact on minorities.

Some states impose a waiting period after felons complete their sentence before they can vote. Few states take the initiative to inform ex-felons when their voting rights are restored. As a result, only a small portion of the ex-felons who have regained their voting rights are registered to vote.

Proponents of re-enfranchisement argue that ex-felons have paid their debt to society when they have completed their full sentence. Restoring their right to vote would encourage them to reintegrate into society. Each state therefore should automatically restore the voting rights of ex-felons who have completed their full sentence, including any terms of parole and compensation to victims. Opponents of re-enfranchisement, however, see this as a "punishment" issue rather than a "voting rights" issue. They believe that each state should be free to decide whether to restore the voting rights of ex-felons. States set punishment for state crimes, and this often extends beyond the completion of a felon's sentence. Ex-felons are, for instance, usually barred from purchasing firearms or from getting a job as a public-school teacher. Nonetheless, weighing both sides of the debate, the Commission believes that voting rights should be restored to certain categories of felons after they served the debt to society.

Recommendations on Re-Enfranchisement of Ex-Felons

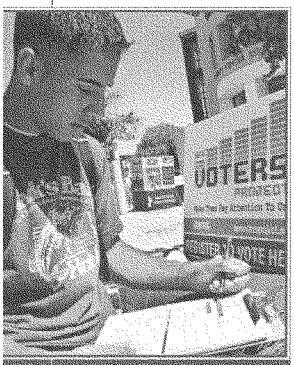
4.6.1 States should allow for restoration of voting rights to otherwise eligible citizens who have been convicted of a felony (other than for a capital crime or one which requires enrollment with an offender registry for sex crimes) once they have fully served their sentence, including any term of probation or parole.

4.6.2 States should provide information on voter registration to ex-felons who have become eligible to vote. In addition, each state's department of corrections should automatically notify the state election office when a felon has regained eligibility to vote.

4.7 VOTER AND CIVIC EDUCATION

Among the simplest ways to promote greater and more informed participation in elections is to provide citizens with basic information on voting and the choices that voters will face in the polling booth. HAVA requires only that basic voter information, including a sample ballot and instructions on how to vote, be posted at each polling site on Election Day. However, additional voter information is needed.

States or local jurisdictions should provide information by mail and on their Web sites to educate voters on the upcoming ballot — on the issues and the candidates, who will provide the information about themselves. Local election officials should set limits on the amount — but not the content — of information to be provided by the candidates. In Washington state, for example, every household is mailed a pamphlet with information on how to register, where to vote, and texts of election laws and proposed ballot initiatives and



A college student in New Mexico registers to vote as part of a campaign to reach new voters. (AP Photo/Luis Chavez Sun-News, Norm Bartlett)

referendums. This voter's pamphlet also has a picture of each candidate for statewide office and a statement of the candidate's goals for the office they seek. In addition, there should be greater use of the radio and television to communicate these messages.

Efforts to provide voter information and education to young Americans merit particular attention. Voter turnout among youth declined steadily from the 1970s to 2000, when it was 24 percent lower than turnout of the entire electorate. In 2004, however, there was a surge of 11 percent in voter turnout among Americans aged 18 to 24, and the gap between youth turnout and overall turnout dropped to 17 percent (see Table 4).[51]

While participation by youth increased significantly in the last election, it continues to lag far behind the rest of the population. It can and should be increased by instructing high school students on their voting rights and civic responsibilities. Just one course in civics or American government can have a strong influence on youth participation in elections. According to a 2003 survey, about twice as many young Americans who have taken a civics course are registered to vote and have voted in all or most elections than young Americans who have never taken such a course.[52]

Moreover, Americans want public schools to prepare their children for citizenship and to provide better civic education. While most Americans believe that the most important goal of public schools is to develop basic skills, seven in 10 respondents to a 2004 survey agreed that preparing students to become responsible citizens is a "central purpose of public schools." When asked to grade the civic education programs of public schools, 54 percent of respondents give these programs a "C" and 22 percent give them a "D."[53]

It is difficult to assess the current efforts of state and local voting and civic education programs because only one state, Florida, publishes a report on its activities and spending in this area. We recommend that more states and local jurisdictions follow Florida's example in order to generate more information on the most effective methods for voter and civic education.

TABLE 4:
Voter Turnout in Presidential Elections by Age, 1972-2004

Age Range	1972	1976	1980	1984	1988	1992	1996	2000	2004
18 to 24 years	49.6	42.2	39.9	40.8	36.2	42.8	32.4	32.3	41.9
25 to 44 years	62.7	58.7	58.7	58.4	54.0	58.3	49.2	49.8	52.2
45 to 64 years	70.8	68.7	69.3	69.8	67.9	70.0	64.4	64.1	66.6
65 years+	63.5	62.2	65.1	67.7	68.8	70.1	67.0	67.6	68.9

SOURCE: U.S. Census Bureau (2004).

Recommendations on Voter and Civic Education

4.7.1 Each state should publish a report on its voter education spending and activities.

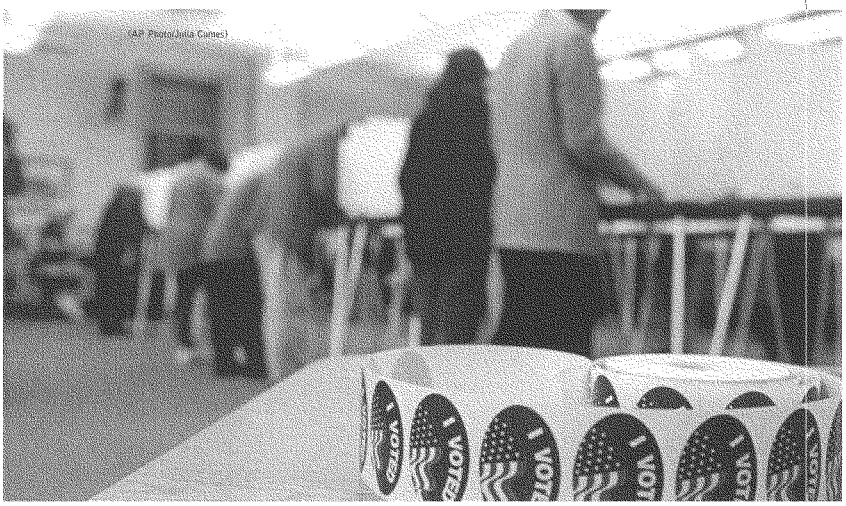
4.7.2 States should engage in appropriate voter education efforts in coordination with local election authorities to assure that all citizens in their state have the information necessary to participate in the election process.

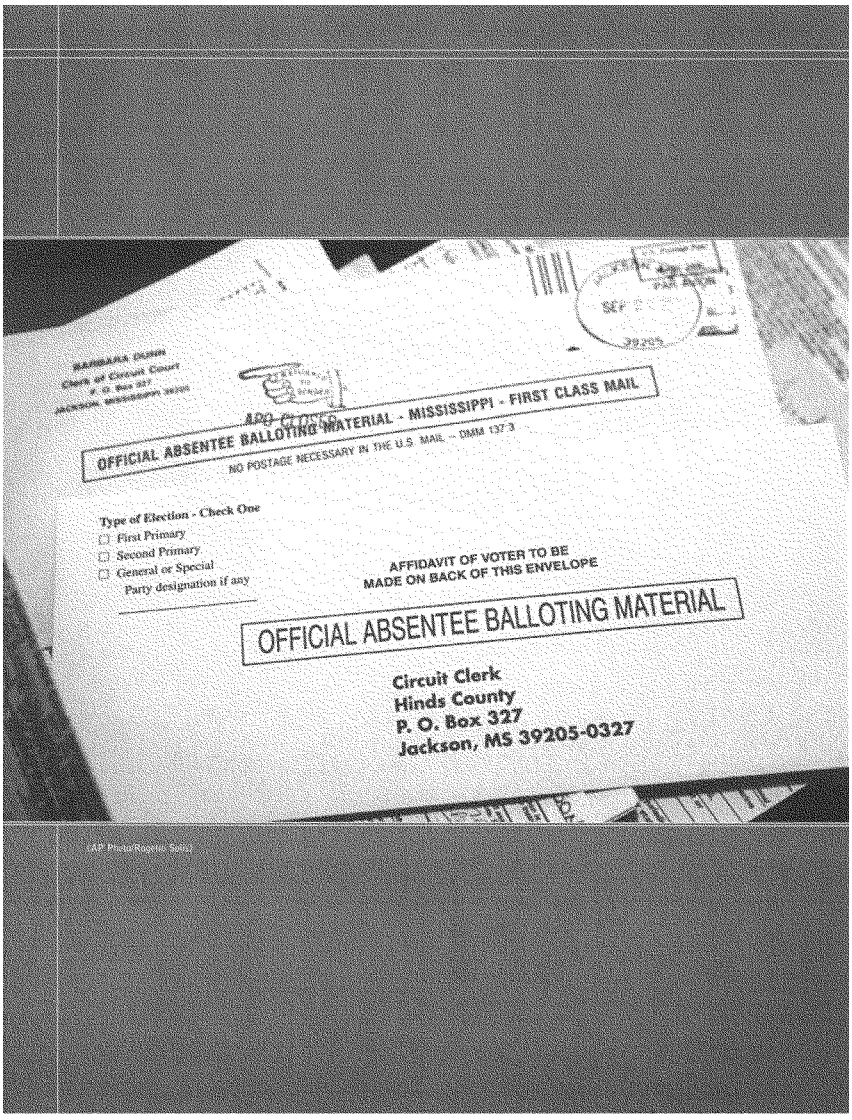
4.7.3 Each state should use its best efforts to instruct all high school students on voting rights and how to register to vote. In addition, civic education programs should be encouraged in the senior year of high school, as these have been demonstrated to increase voter participation by youth.

4.7.4 Local election authorities should mail written notices to voters in advance of an election advising the voter of the date and time of the election and the polling place where the voter can cast a ballot and encouraging the citizens to vote. The notice should also provide a phone number for the voter to contact the election authorities with any questions.

4.7.5 States should mail pamphlets to voters, and post the pamphlet material on their Web sites, to provide information about the candidates for statewide office and about ballot initiatives and referenda.

4.7.6 The federal government should provide matching funds for the states to encourage civic and voter education and advertisements aimed to encourage people to vote.





(AP Photo/Rogelio Solis)

5. Improving Ballot Integrity

Because the integrity of the ballot is a hallmark of democracy, it is imperative that election officials guarantee eligible voters the opportunity to vote, but only once, and tabulate ballots in an accurate and fair manner.

5.1 INVESTIGATION AND PROSECUTION OF ELECTION FRAUD

While election fraud is difficult to measure, it occurs. The U.S. Department of Justice has launched more than 180 investigations into election fraud since October 2002. These investigations have resulted in charges for multiple voting, providing false information on their felon status, and other offenses against 89 individuals and in convictions of 52 individuals. The convictions related to a variety of election fraud offenses, from vote buying to submitting false voter registration information and voting-related offenses by non-citizens.[54]

In addition to the federal investigations, state attorneys general and local prosecutors handle cases of election fraud. Other cases are never pursued because of the difficulty in obtaining sufficient evidence for prosecution or because of the low priority given to election fraud cases. One district attorney, for example, explained that he did not pursue allegations of fraudulent voter registration because that is a victimless and nonviolent crime.[55]

Election fraud usually attracts public attention and comes under investigation only in close elections. Courts may only overturn an election result if there is proof that the number of irregular or fraudulent votes exceeded the margin of victory. When there is a wide margin, the losing candidate rarely presses for an investigation. Fraud in any degree and in any circumstance is subversive to the electoral process. The best way to maintain ballot integrity is to investigate all credible allegations of election fraud and otherwise prevent fraud before it can affect an election.

Investigation and prosecution of election fraud should include those acts committed by individuals, including election officials, poll workers, volunteers, challengers or other nonvoters associated with the administration of elections, and not just fraud by voters.

Recommendations on Investigation and Prosecution of Election Fraud

5.1.1 In July of even-numbered years, the U.S. Department of Justice should issue a public report on its investigations of election fraud. This report should specify the numbers of allegations made, matters investigated, cases prosecuted, and individuals convicted for various crimes. Each state's attorney general and each local prosecutor should issue a similar report.

5.1.2 The U.S. Department of Justice's Office of Public Integrity should increase its staff to investigate and prosecute election-related fraud.

5.1.3 In addition to the penalties set by the Voting Rights Act, it should be a federal felony for any individual, group of individuals, or organization to engage in any act of violence, property destruction (of more than $500 value), or threatened act of violence that is intended to deny any individual his or her lawful right to vote or to participate in a federal election.

5.1.4 To deter systemic efforts to deceive or intimidate voters, the Commission recommends federal legislation to prohibit any individual or group from deliberately providing the public with incorrect information about election procedures for the purpose of preventing voters from going to the polls.

5.2 ABSENTEE BALLOT AND VOTER REGISTRATION FRAUD

Fraud occurs in several ways. Absentee ballots remain the largest source of potential voter fraud.[16] A notorious recent case of absentee ballot fraud was Miami's mayoral election of 1998, and in that case, the judge declared the election fraudulent and called for a new election. Absentee balloting is vulnerable to abuse in several ways: Blank ballots mailed to the wrong address or to large residential buildings might get intercepted. Citizens who vote at home, at nursing homes, at the workplace, or in church are more susceptible to pressure, overt and subtle, or to intimidation. Vote buying schemes are far more difficult to detect when citizens vote by mail. States therefore should reduce the risks of fraud and abuse in absentee voting by prohibiting "third-party" organizations, candidates, and political party activists from handling absentee ballots. States also should make sure that absentee ballots received by election officials before Election Day are kept secure until they are opened and counted.

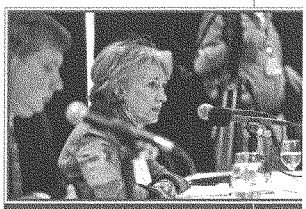
Non-citizens have registered to vote in several recent elections. Following a disputed 1996 congressional election in California, the Committee on House Oversight found 784 invalid votes from individuals who had registered illegally. In 2000, random checks by the Honolulu city clerk's office found about 200 registered voters who had admitted they were not U.S. citizens.[17] In 2004, at least 35 foreign citizens applied for or received voter cards in Harris County, Texas, and non-citizens were found on the voter registration lists in Maryland as well.[18]

The growth of "third-party" (unofficial) voter registration drives in recent elections has led to a rise in reports of voter registration fraud. While media attention focused on reports of fraudulent voter registrations with the names of cartoon characters and dead people, officials in 10 states investigated accusations of voter registration fraud stemming from elections in 2004, and between October 2002 and July 2005, the U.S. prosecuted 19 people charged with voter registration fraud.[19] Many of these were submitted by third-party organizations, often by individuals who were paid by the piece to register voters.

States should consider new legislation to minimize fraud in voter registration, particularly to prevent abuse by third-party organizations that pay for voter registration by the piece. Such legislation might direct election offices to check the identity of individuals registered through third-party voter registration drives and to track the voter registration forms.

HAVA requires citizens who register by mail to vote in a state for the first time to provide

an ID when they register or when they vote. Some states have interpreted this requirement to apply only to voter registration forms sent to election offices by mail, not to forms delivered by third-party organizations. As a result, neither the identity nor the actual existence of applicants is verified. All citizens who register to vote with a mail-in form, whether that form is actually sent by mail or is instead hand-delivered, should comply with HAVA's requirements or with stricter state requirements on voter ID, by providing proof of identity either with their registration application or when they appear at the polling station on Election Day. In this way, election offices will be obliged to verify the identity of every citizen who registers to vote, whether or not the registration occurs in person.



John Fund and Colleen McAndrews at the April 19 hearing (American University Photo/Jeff Watts)

In addition, states should introduce measures to track voter registration forms that are handled by third-party organizations. By assigning a serial number to all forms, election officials will be able to track the forms. This, in turn, will help in any investigations and prosecutions and thus will serve to deter voter registration fraud.

Many states allow the representatives of candidates or political parties to challenge a person's eligibility to register or vote or to challenge an inaccurate name on a voter roll. This practice of challenges may contribute to ballot integrity, but it can have the effect of intimidating eligible voters, preventing them from casting their ballot, or otherwise disrupting the voting process. New procedures are needed to protect voters from intimidating tactics while also offering opportunities to keep the registration rolls accurate, and to provide observers with meaningful opportunities to monitor the conduct of the election. States should define clear procedures for challenges, which should mainly be raised and resolved before the deadline for voter registration. After that, challengers will need to defend their late actions. On Election Day, they should direct their concerns to poll workers, not to voters directly, and should in no way interfere with the smooth operation of the polling station.

Recommendations on Absentee Ballot and Voter Registration Fraud

5.2.1 State and local jurisdictions should prohibit a person from handling absentee ballots other than the voter, an acknowledged family member, the U.S. Postal Service or other legitimate shipper, or election officials. The practice in some states of allowing candidates or party workers to pick up and deliver absentee ballots should be eliminated.

5.2.2 All states should consider passing legislation that attempts to minimize the fraud that has resulted from "payment by the piece" to anyone in exchange for their efforts in voter registration, absentee ballot, or signature collection.

5.2.3 States should not take actions that discourage legal voter registration or get-out-the-vote activities or assistance, including assistance to voters who are not required to vote in person under federal law.



(AP Photo/D. Pat Carter)

6. Election Administration

To build confidence in the electoral process, it is important that elections be administered in a neutral and professional manner. Election officials, from county clerks and election board members to secretaries of state and U.S. Election Assistance Commission members, generally have shown great skill and dedication in administering elections in a fair and impartial manner. The institutions of election administration, however, are in need of improvement, so that they may instill greater public confidence in the election process and allow election officials to carry out their responsibilities more effectively (see Table 5 on page 52).

Elections are contests for power and, as such, it is natural that politics will influence every part of the contest, including the administration of elections. In recent years, some partisan election officials have played roles that have weakened public confidence in the electoral process. Many other partisan election officials have tried to execute their responsibilities in a neutral manner, but the fact that they are partisan sometimes raises suspicions that they might favor their own party. Most other democratic countries have found ways to insulate electoral administration from politics and partisanship by establishing truly autonomous, professional, and nonpartisan independent national election commissions that function almost like a fourth branch of government. The United States, too, must take steps to conduct its elections impartially both in practice and in appearance.

Impartial election administration, however, is not enough. Elections must also be administered effectively if they are to inspire public confidence. Long lines at polling stations, inadequately trained poll workers, and inconsistent or incorrect application of electoral procedures may have the effect of discouraging voter participation and may, on occasion, raise questions about bias in the way elections are conducted. While problems at polling stations usually reflect a shortage of trained poll workers or poor management of polling station operations, rather than an attempt to seek partisan advantage, the result is much the same. Such problems raise public suspicions or may provide grounds for the losing candidate to contest the result in a close election.

6.1 INSTITUTIONS

The intense partisanship and the close division of the American electorate, coupled with the Electoral College system, raise the possibility of another presidential election decided by a razor-thin margin in one or more battleground states. Although voting technology is improving, presidential elections are held in a decentralized system with a patchwork of inconsistent rules. In addition, in recent years, election challenges in the courts have proliferated.

Close elections, especially under these conditions, put a strain on any system of election administration, and public opinion demonstrates this. Significant segments of the American public have expressed concern about voter fraud, voter suppression, and the fairness of the election process in general.[60] While substantially more Democrats than Republicans surveyed in national polls considered the 2004 presidential election unfair, 41 percent more Republicans than Democrats said the electoral process was unfair in Washington state's 2004 gubernatorial election, which the Democratic candidate won by a very narrow margin.[61] The losing side, not surprisingly, is unhappy with the election result, but what is new and dangerous in the United States is that the supporters of the losing side are beginning to believe that the process is unfair. And this is true of both parties.

At its base, the problem is a combustible mixture of partisan suspicion and irregularities born in part from a decentralized system of election administration with differing state laws determining voter registration and eligibility and whether a ballot is actually counted. The irregularities, by and large, stem from a lack of resources and inadequate training for election workers, particularly those who work just on Election Day. In other countries, such irregularities sometimes lead to street protests or violence. In the United States, up until now, we have been relatively fortunate that irregularities are addressed in court. The dramatic increase in election-related litigation in recent years, however, does not enhance the public's perception of elections and may in fact weaken public confidence. The average number of election challenges per year has increased from 96 in the period of 1996 to 1999 to 254 in 2001 to 2004.[62]



Elections manager Lori Augino, left, Pierce County Auditor Pat McCarthy, U.S. EAC Commissioners Ray Martinez, III, and Paul DeGregorio, right, observe the 2004 manual gubernatorial recount in Washington (AP Photo/*The News Tribune*, Janet Jensen)

Another major source of public mistrust of the election process is the perception of partisanship in actions taken by partisan election officials. In a majority of states, election administration comes under the authority of the secretary of state. In 2000 and 2004, both Republican and Democratic secretaries of state were accused of bias because of their discretionary decisions — such as how to interpret unclear provisions of HAVA. The issue is not one of personality or a particular political party because allegations and irregularities dogged officials from both parties. The issue is the institution and the perception of partiality that is unavoidable if the chief election officer is a statewide politician and the election is close, has irregularities, or is disputed. The perception of partiality is as important, if not more so, than the reality.

Bipartisan election administration has the advantage of allowing both parties to participate, but the flaws of such a system are evident in the experience of the Federal Election Commission (FEC). The FEC has often become deadlocked on key issues. In the cases when the FEC commissioners agree, they sometimes protect the two parties from enforcement rather than represent the public's interest in regulating campaign finance.

NONPARTISAN ELECTION ADMINISTRATION. To minimize the chance of election meltdown and to build public trust in the electoral process, nonpartisan structures of election administration are very important, and election administrators should be neutral, professional, and impartial. At the federal level, the U.S. Election Assistance Commission should be reconstituted on a nonpartisan basis to exercise whatever powers are granted by law, and the EAC chairperson should serve as a national spokesperson, as the chief elections officer in Canada does, for improving the electoral process. States should consider transferring the authority for conducting elections from the secretary of state to a chief election officer, who would serve as a nonpartisan official.

States could select a nonpartisan chief elections officer by having the individual subject to approval by a super-majority of two-thirds of one or both chambers of the state legislature. The nominee should receive clear bipartisan support. This selection process is likely to yield a respected consensus candidate or, at least, a nonpartisan candidate.

The EAC, in its 18 months of operation, has managed to make its decisions by consensus. While this is a significant accomplishment for a bipartisan, four-member commission, it has come at a cost. The EAC has been slow to issue key guidance, and the guidance it has issued has often been vague. The process of forging consensus among the EAC's commissioners appears to have slowed and watered down key decisions, particularly as they have come under pressure from their respective political parties. If the EAC were reconstituted as a nonpartisan commission, it would be better able to resist partisan political pressure and operate more efficiently and effectively.

To avoid the dangers of bipartisan stalemate, the EAC should be reconstituted as a five-member commission, with a strong chairperson and nonpartisan members. This would be done initially by adding a fifth position to the EAC and making that position the chairperson, when the current chairperson's term ends. The new EAC chairperson would be nonpartisan, nominated by the President, and confirmed by the U.S. Senate. Later, as the terms of other EAC commissioners expired, they would be replaced by nonpartisan commissioners, subject to Senate confirmation as well.



Kansas Secretary of State Ron Thornburgh at the April 18 hearing (American University Photo/Jeff Watts)

INDEPENDENCE AND AUTHORITY. For the positions of EAC commissioners and state chief elections officers to remain both nonpartisan and effective, they must be insulated from political pressure. This can be done by the terms of appointment and the lines of responsibility. The EAC commissioners and state chief elections officers should receive a long-term appointment, perhaps 10 years. The grounds for dismissal should be limited, similar to the rules for removal of a federal or state judge. The EAC should have the autonomy to oversee federal election laws that Congress directs it to implement and advise Congress and the President on needed improvements in election systems. State chief elections officers should have similar autonomy.

Under HAVA, the EAC distributes federal funds to the states, issues voluntary guidance on HAVA's mandates, and serves as a clearinghouse for information on elections. In addition, it develops standards for voting equipment and undertakes research on elections.

The flaws identified in the electoral system described in this report were due in large part to a very decentralized system with voting standards implemented in different ways throughout the country. If HAVA is fully and effectively implemented, states should be able to retrieve authority to conduct elections from counties and impose a certain degree of uniformity.

In this report, we have proposed the kinds of reforms needed to improve significantly our electoral process. To implement those reforms, a new or invigorated institution like the EAC is needed to undertake the following tasks:

- Statewide registration lists need to be organized top-down with states in charge and counties assisting states rather than the other way around;
- A template and a system is needed for sharing voter data across states;

- The "REAL ID" needs to be adapted for voting purposes and linked to the registration list;
- To ensure that the new requirements — ID and registration list — do not impede access to voting, an expanded effort is needed to reach out and register new voters;
- Quality audits of voter databases and certification of voting machine source codes is essential;
- Voting machines need a voter-verifiable audit trail; and
- Extensive research on the operations and technology of elections is needed.

TABLE 5: Types of Electoral Administration

Type of Institution	WORLD REGION: The Americas	Asia & the Pacific	East & Central Europe	Sub-Saharan Africa	Total Number of Cases (percent of total)
Government	5*	9	0	3	17 (14%)
Government supervised by judges or others	6	2	6	14	28 (23%)
Independent electoral commission	25	19	12	19	75 (63%)

* The U.S. is included in this category.

SOURCE: Rafael López-Pintor. *Electoral Management Bodies as Institutions of Governance* (NY: United Nations Development Programme, Bureau for Development Policy, 2000).

These reforms, but particularly those that require connecting states, will not occur on their own. The EAC needs to have sufficient authority to assure effective and consistent implementation of these reforms, and to avoid repeating past problems, its guidance must be clear and compelling. A stronger EAC does not mean that the states will lose power in conducting elections. To the contrary, the authority of state election officials will grow with the creation of statewide voter databases, and their credibility will be enhanced by the new nonpartisan structure and professionalism.

CONFLICT-OF-INTEREST RULES. No matter what institutions are responsible for conducting elections, conflict-of-interest standards should be introduced for all federal, state, and local election officials, including some of the provisions in Colorado's new election law and of the Code of Conduct prepared by the International Institute for Democracy and Electoral Assistance (IDEA).[63] This Code of Conduct requires election administrators to avoid any activity, public or private, that might indicate support or even sympathy for a particular candidate, political party, or political tendency.

Election officials should be prohibited by federal and/or state laws from serving on any political campaign committee, making any public comments in support of a candidate, taking a public position on any ballot measure, soliciting campaign funds, or otherwise campaigning for or against a candidate for public office. A decision by a secretary of state to serve as co-chair of his or her party's presidential election committee would clearly violate these standards.

Recommendations on Institutions

6.1.1 To undertake the new responsibilities recommended by this report and to build confidence in the administration of elections, Congress and the states should reconstitute election management institutions on a nonpartisan basis to make them more independent and effective. U.S. Election Assistance Commission members and each state's chief elections officer should be selected and be expected to act in a nonpartisan manner, and the institutions should have sufficient funding for research and training and to conduct the best elections possible. We believe the time has come to take politics as much as possible out of the institutions of election administration and to make these institutions nonpartisan.

6.1.2 Congress should approve legislation that would add a fifth member to the U.S. Election Assistance Commission, who would serve as the EAC's chairperson and who would be nominated by the President based on capability, integrity, and nonpartisanship. This would permit the EAC to be viewed more as nonpartisan than bipartisan and would improve its ability to make decisions. That person would be subject to Senate confirmation and would serve a single term of ten years. Each subsequent vacancy to the EAC should be filled with a person judged to be nonpartisan so that after a suitable period, all the members, and thus the institution, might be viewed as above politics.

6.1.3 States should prohibit senior election officials from serving or assisting political campaigns in a partisan way, other than their own campaigns in states where they are elected.

6.1.4 States should take additional actions to build confidence in the administration of elections by making existing election bodies as nonpartisan as possible within the constraints of each state's constitution. Among the ways this might be accomplished would be if the individuals who serve as the state's chief elections officer were chosen based on their capability, integrity, and nonpartisanship. The state legislatures would need to confirm these individuals by a two-thirds majority of one or both houses. The nominee should receive clear bipartisan support.

6.1.5 Each state's chief elections officer should, to the extent reasonably possible, ensure uniformity of voting procedures throughout the state, as with provisional ballots. Doing so will reduce the likelihood that elections are challenged in court.

6.2 POLL WORKER RECRUITMENT

For generations, civic-minded citizens, particularly seniors, have served as poll workers. The average age of poll workers is 72.[64] Poll workers generally are paid minimum wages for a 15-hour day. Not surprisingly, recruitment has proven more and more difficult. For the 2004 election, the United States needed 2 million poll workers, but it fell short by 500,000.

Effective administration of elections requires that poll workers have the capability and training needed to carry out complex procedures correctly, the skills to handle increasingly sophisticated voting technology, the personality and skills to interact with a diversity of people in a calm and friendly manner, and the energy to complete a very long and hard day of work on Election Day. Poll workers must administer complex voting procedures, which are often changed with each election. These procedures include issuing provisional ballots, checking voter identification in accordance with state law, and correctly counting the votes after the polling station closes. Poll workers must also set up voting machines, instruct voters to use these machines, and provide helpful service to voters, including to voters with disabilities and non-English speakers.



Commissioner Sharon Priest, Daniel Calingaert, Michael Alvarez, and Election Center Executive Director Doug Lewis. (Rice University Photo/Jeff Fitlow)

A broad pool of potential recruits, drawn from all age groups, is needed to meet the demands made on today's poll workers. To adequately staff polling stations, states and local jurisdictions must offer better pay, training, and recognition for poll workers and recruit more citizens who have full-time jobs or are students. Recruitment of teachers would serve to spread knowledge of the electoral process, while recruitment of students would educate future voters and attract individuals who may serve as poll workers for decades to come.

Local election authorities should also consider providing incentives for more rigorous training. Guilford County, North Carolina, for example, initiated a "Precinct Officials Certification" program in cooperation with the local community college. The program requires 18 hours of class and a final exam. While voluntary, more than 80 percent of Guilford County's 636 permanent precinct officials completed the course. Certified officials receive an additional $35 per election in pay. Retention of officials has risen from roughly 75 percent to near 95 percent.

In addition, poll workers deserve greater recognition for their public service. States might establish a Poll Worker Appreciation Week and issue certificates to thank poll workers for their contribution to the democratic process.

Several states have passed laws to provide paid leave for state and local government workers who serve as poll workers on Election Day. A pilot program titled "Making Voting Popular" was implemented in 1998 in six counties surrounding the Kansas City metropolitan area to encourage employers to provide a paid "civic leave" day for employees who work as poll workers. Many states have introduced laws to encourage the recruitment of student poll workers. Partnered with experienced poll workers, student poll workers can learn about elections while contributing their technological skills.

It will be easier to recruit skilled poll workers if they are given flexibility in the terms of their service by working part of the day. Since a large proportion of voters arrive either at the beginning or the end of the day, it would make sense to hire more poll workers for those periods, although this is not now the case. Bringing poll workers in from other jurisdictions might also serve to provide partisan balance in jurisdictions where one party is dominant. Flexibility in the terms of service by poll workers is often restricted by state laws. Where this is the case, states should amend their laws to allow part-day shifts for poll workers on Election Day and to permit state residents to staff polling stations in a different jurisdiction.

In addition, states might consider a new practice of recruiting poll workers in the same way that citizens are selected for jury duty. This practice is used in Mexico, where citizens are selected randomly to perform what they consider a civic obligation. About five times as many poll workers as needed are trained in Mexico, so that only the most skilled and committed are selected to serve as poll workers on Election Day. The process of training so many citizens serves the additional purpose of educating the public in voting procedures. This practice both reflects and contributes to a broad civic commitment to democracy.

Recommendations on Poll Worker Recruitment

6.2.1 States and local jurisdictions should allocate sufficient funds to pay poll workers at a level that would attract more technologically sophisticated and competent workers. Part-time workers should also be recruited for the beginning and the end of Election Day. States should amend their laws to allow shifts for part of the day for poll workers on Election Day.

6.2.2 States and local jurisdictions should implement supplemental training and recognition programs for poll workers.

6.2.3 To increase the number and quality of poll workers, the government and nonprofit and private employers should encourage their workers to serve as poll workers on Election Day without any loss of compensation, vacation time or personal time off. Special efforts should be made to enlist teachers and students as poll workers.

6.2.4 Because some jurisdictions have large majorities of one party, which makes it hard to attract poll workers from other parties, local jurisdictions should allow poll workers from outside the jurisdiction.

6.2.5 States should consider legislation to allow the recruitment of citizens as poll workers as is done for jury duty.



Long line of Ohio voters on Election Day 2004
(AP Photo/Mark Duncan)

6.3 POLLING STATION OPERATIONS

A visible problem on Election Day 2004 was long lines. This should have been anticipated because there was a surge in new registrations and people expected a close election, particularly in "battleground states." Still, too many polling stations were unprepared. While waiting until 4 a.m. to vote was an extreme case, too many polling stations experienced long lines at the beginning of the day when people went to work or at the day's end when they returned. Fast-food chains hire extra workers at lunchtime, but it apparently did not occur to election officials to hire more workers at the times when most people vote. Long lines were hardly the only problem; many polling stations had shortages of provisional ballots, machines malfunctioned, and there were too many inadequately trained workers on duty. Although most states ban campaigning within a certain distance of a polling station, other states or counties permit it, though many voters find it distasteful if not intimidating.

Problems with polling station operations, such as long lines, were more pronounced in some places than in others.[65] This at times gave rise to suspicions that the problems were due to discrimination or to partisan manipulation, when in fact the likely cause was a poor decision by election administrators. The U.S. Department of Justice's investigation into the allocation of voting machines in Ohio, for example, found that problems were due to administrative miscalculations, not to discrimination.[66]

The 2004 elections highlighted the importance of providing enough voting machines to each polling place. While voter turnout can be difficult to predict, the ratio of voters per machine can be estimated. Texas, for example, has issued an administrative rule to estimate the number of machines needed per precinct at different rates of voter turnout.[67]

The impression many voters get of the electoral process is partially shaped by their

experience at the polling station, and yet, not enough attention has been given to trying to make them "user-friendly." Elementary questions, which most businesses study to become more efficient and responsive to their customers, are rarely asked, let alone answered by election officials. Questions like: How long does it normally take for a citizen to vote? Would citizens prefer to go to a neighborhood precinct, or to a larger, more service-oriented but more distant "voting center"? How many and what kinds of complaints and problems do polling stations hear in an average day? How do they respond, and are voters satisfied with the response? How many citizens find electronic machines useful, and how many find them formidable? By answering these fundamental questions, we might determine ways to provide efficient and courteous service at polling locations

A simple way to compile useful information about problems voters face on Election Day would be to require that every voting station maintain a "log book" on Election Day to record all complaints from voters or observers. The log book would be signed by election observers at the end of the day to make sure that it has recorded all the complaints or problems. An analysis of the log books would help identify common problems and help design more efficient and responsive polling sites.

Recommendations on Polling Station Operations

6.3.1 Polling stations should be made user-friendly. One way to do so would be to forbid any campaigning within a certain distance of a polling station.

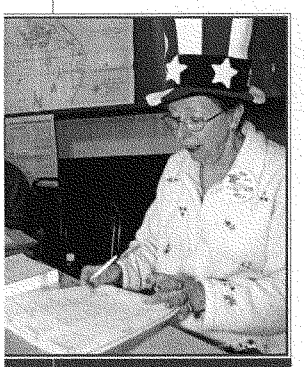
6.3.2 Polling stations should be required to maintain a "log-book" on Election Day to record all complaints. The books should be signed by election officials and observers and analyzed for ways to improve the voting process.

6.3.3 Polling stations should be organized in a way that citizens would not have to wait long before voting, and officials should be informed and helpful.

6.4 RESEARCH ON ELECTION MANAGEMENT

Despite the wealth of expertise and literature on U.S. elections and voting behavior, little research focuses on the administration or conduct of elections. Until the 2000 election stirred interest in the subject, we had no information on how often votes went uncounted. Today, we still do not know how many people are unable to vote because their name is missing from the registration list or their identification was rejected at the polls. We also have no idea about the level of fraud or the accuracy and completeness of voter registration lists.

To effectively address the challenges facing our election systems, we need to understand better how elections are administered. The log books and public reports on investigations on election fraud, described above, can provide some good raw material. But we need more systematic research to expand knowledge and stimulate needed improvements in U.S. election systems. Moreover, beyond the reforms needed today, U.S. election systems will need to adapt in the future to new technology and to social changes.



A North Dakota election judge on Election Day 2004. (AP Photo/Will Kincaid)

The Center for Election Systems at Kennesaw State University in Georgia is the first university center established to study election systems and to assist election administration. With funding from the state government, this Center develops standards for voting technology used in Georgia and provides an array of other services, such as testing all election equipment, providing training, building databases, and designing ballots for many counties. The Center thus provides critical services to state election authorities and supports constant improvements in election systems. Since election laws and procedures vary significantly, each state should consider supporting university centers for the study of elections.

In addition to research on technology, university election centers could assist state governments on issues of election law, management, and civic and voter education. They could assemble experts from different disciplines to assist state governments in reviewing election laws, improving administrative procedures, strengthening election management, and developing programs and materials to train poll workers.

Comparative research is also needed on electoral systems in different states, and national studies should be conducted on different elements of election administration and causes of voter participation. These studies might address such questions as: What factors stimulate or depress participation in elections? How do voters adapt to the introduction of new voting technologies? And what are the costs of conducting elections? Research on these and a host of other questions is needed at the national, state, and local levels, with findings shared and efforts coordinated. Moreover, federal, state, and private foundation funds are needed to generate the research our election systems require to effectively inform decision-making, to monitor and advance best practices, and to measure implementation and enforcement.[68]

Recommendation on Research on Election Management

6.4.1 The Commission calls for continuing research on voting technology and election management so as to encourage continuous improvements in the electoral process.

6.5 COST OF ELECTIONS

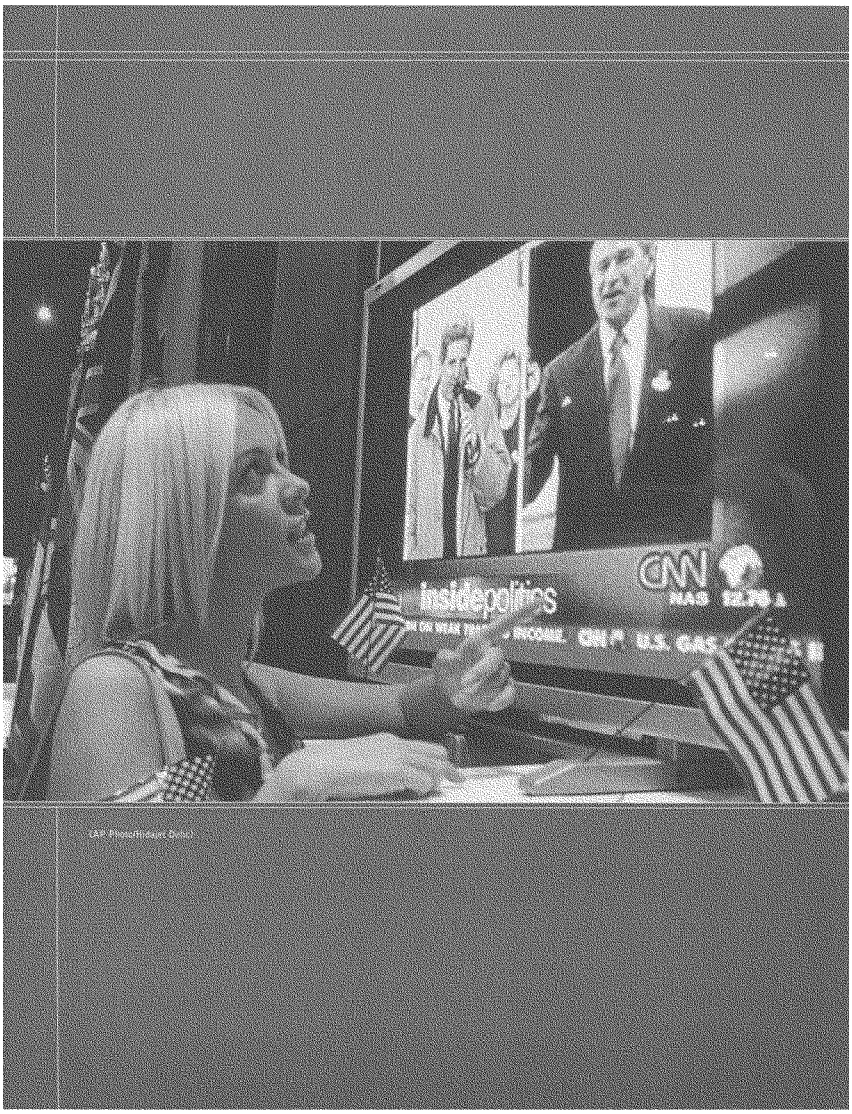
Based on the limited available information, the cost of elections appears to vary significantly by state. Wyoming, for example, spent $2.15 per voter for the 2004 elections, while California spent $3.99 per voter.[69] Information on the cost of elections is difficult to obtain, because both state and local authorities are involved in running elections, and local authorities often neglect to track what they spend on elections. At the county level, elections typically are run by the county clerk and recorder, who rarely keeps track of the staff time and office resources allocated to elections as opposed to other office responsibilities.

Election administration expenditures in the United States are on the low end of the range of what advanced democracies spend on elections. Among advanced democracies, expenditures on election administration range from lows of $2.62 in the United Kingdom and $3.07 in France for national legislative elections, through a midrange of $4.08 in Spain and $5.68 in Italy, to a high of $9.30 in Australia and $9.51 in Canada.[70] While larger expenditures provide no guarantee of greater quality in election administration, they tend to reflect the priority given to election administration. The election systems of Australia and Canada are the most expensive but are also considered among the most effective and modern election systems in the world. Both local and state governments should track and report the cost of elections per registered voter. This data would be very important in offering comparisons on alternative and convenience voting.

Recommendations on Cost of Elections

6.5.1 As elections are a bedrock of our nation's democracy, they should receive high priority in the allocation of government resources at all levels. Local jurisdictions, states, and the Congress should treat elections as a high priority in their budgets.

6.5.2 Both local and state governments should track and report the cost of elections per registered voter.


CNN
insidepolitics
U.S. GAS

7. Responsible Media Coverage

The media's role in elections is of great consequence. Effective media coverage contributes substantially to the electoral process by informing citizens about the choices they face in the elections and about the election results. In contrast, irresponsible media coverage weakens the quality of election campaigns and the public's confidence in the electoral process.

7.1 MEDIA ACCESS FOR CANDIDATES

More than $1.6 billion was spent on television ads in 2004 by candidates, parties, and independent groups.[71] This was a record for any campaign year and double the amount spent in the 2000 presidential election.

The pressure to raise money to pay for TV ads has tilted the competitive playing field in favor of well-financed candidates and has created a barrier to entry in politics. Moreover, TV ads tend to reduce political discourse to its least attractive elements—campaign spots are often superficial and negative. This has a significant impact on the quality of campaigns, as television is the primary source of campaign information for about half of all Americans.[72]

Broadcasters receive free licenses to operate on our publicly owned airwaves in exchange for a pledge to serve the public interest. At the heart of this public interest obligation is the need to inform the public about the critical issues that will be decided in elections.

In 1998, a White House advisory panel recommended that broadcasters voluntarily air at least five minutes of candidate discourse every night in the month preceding elections. The goal of this "5/30 standard" was to give television viewers a chance to see candidates in nightly forums that are more substantive than the political ads that flood the airwaves in the final weeks of election campaigns. National networks were encouraged to broadcast a nightly mix of interviews, mini-debates, and issue statements by presidential candidates, and local stations were asked to do the same for candidates in federal, state, and local races. Complete editorial control over the forums for candidate discourse was, of course, left to the national networks and local stations, which would decide what campaigns to cover, what formats to use, and when to broadcast the forums.

In 2000, about 103 television stations pledged to provide at least five minutes of campaign coverage every night in the final month of the election campaign, yet they often fell short of the 5/30 standard. Local news broadcasts of these 5/30 stations provided coverage, on average, of only two minutes and 17 seconds per night of candidate discourse.[73] On the thousand-plus stations that did not pledge to meet the 5/30 standard, coverage of candidate discourse was minimal.

During the 2004 campaign, substantive coverage of candidate discourse was still modest:[74]

- Little attention was given to state and local campaigns. About 92 percent of the election coverage by the national television networks was devoted to the presidential race. Less than 2 percent was devoted to U.S. House or U.S. Senate races.

- The presidential campaign also dominated local news coverage, but the news focuses on the horse race between candidates rather than on important

issues facing Americans. While 55 percent of local news broadcasts contained a story about the presidential election, only 8 percent had one about a local race. About 44 percent of the campaign coverage focused on campaign strategy, while less than one-third addressed the issues.

- Local campaign coverage was dwarfed by other news. Eight times more local broadcast coverage went to stories about accidental injuries, and 12 times more coverage went to sports and weather than to all local races combined.

- Only 24 percent of the local TV industry pledged to meet the "5/30" standard.

Notwithstanding the dramatic expansion of news available on cable television, broadcasters can and should do more to improve their coverage of campaign issues. Some propose to require broadcasters to provide free air time to candidates, but others are concerned that it might lead toward public financing of campaigns or violate the First Amendment.

Recommendations on Media Access for Candidates

7.1.1 The Commission encourages national networks and local TV stations to provide at least five minutes of candidate discourse every night in the month leading up to elections.

7.1.2 The Commission encourages broadcasters to continue to offer candidates short segments of air time to make issue statements, answer questions, or engage in mini-debates.

7.1.3 Many members of the Commission support the idea that legislation should be passed to require broadcasters to give a reasonable amount of free air time to political candidates, along the lines of the provisions of the Our Democracy, Our Airwaves Act of 2003 (which was introduced as S.1497 in the 108th Congress).

7.2 MEDIA PROJECTIONS OF ELECTION RESULTS

For decades, early projections of presidential election results have diminished participation in the electoral process. Projections of Lyndon Johnson's victory in 1964 came well before the polls closed in the West. The same occurred in 1972 and in 1980. In all of these cases, candidates further down the ballot felt the effect. In 1980, the estimated voter turnout was about 12 percent lower among those who had heard the projections and not yet voted as compared with those who had not heard the projections.[75]

On Election Night in 2000, the major television news organizations — ABC, CBS, NBC, CNN, and Fox — made a series of dramatic journalistic mistakes. While polls were still open in Florida's panhandle, they projected that Vice President Gore had won the state. They later reversed their projection and predicted that Governor Bush would win Florida and, with it, the presidency. Gore moved to concede the election, beginning with a call to Bush. Gore later withdrew his concession, and the news organizations had to retract their projection of Bush's victory. The first set of mistakes may have influenced voters in Florida and in other states where the polls were still open. The second set of mistakes irretrievably influenced public perceptions of the apparent victor in the election, which then affected the subsequent controversy over the outcome in Florida.

Having made these mistakes in 2000, most television news organizations were cautious about projecting presidential election results in 2004. This caution is worth repeating in future elections and should become a standard media practice.

The Carter-Ford Commission was highly critical of the practice of declaring a projected winner in a presidential election before all polls close in the contiguous 48 states of the United States. In the Commission's view, this practice discourages voters by signaling that the election is over even before some people vote.

Voluntary restraint by major media organizations is a realistic option. National news networks in the last several presidential elections have voluntarily refrained from calling the projected presidential winner in the Eastern Standard Time zone until after 7:00 p.m. (EST). In addition, as a result of the mistakes they made in 2000, the networks have now agreed to refrain from calling the projected presidential winner in states with two time zones until all of the polls across the state have closed.

Media organizations should exercise similar restraint in their release of exit poll data. The Carter-Ford Commission noted the mounting body of evidence that documents the unreliability of exit polls. In 2000, exit polls conflicted with the actual election results in many states — and in five specific instances by as much as 7 percent to 16 percent. Network news organization officials acknowledged that exit polls have become more fallible over the years as more and more voters have refused to take part. In 2000, only about half of the voters asked to participate in exit polls agreed to do so, and only 20 percent of absentee and early voters agreed to participate in telephone "exit" poll interviews. That response rate is too low to assure reliability in exit polls.

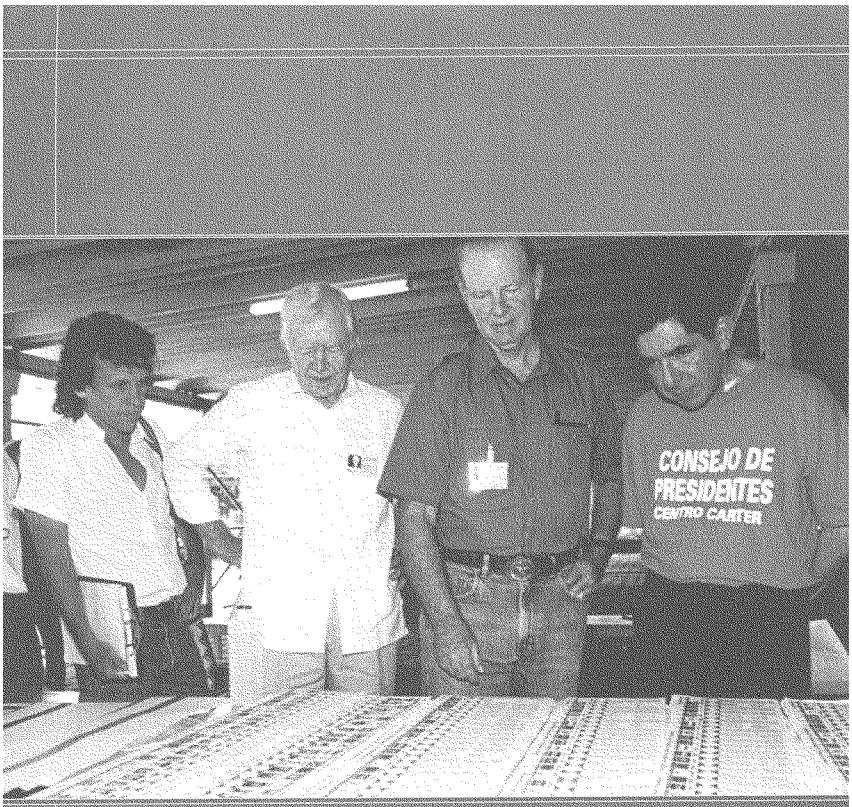
Despite the effort made to improve exit polls for the 2004 presidential election, they were well off the mark and misled some Americans about the election's outcome. By now it should be abundantly clear that exit polls do not reliably predict election results. While exit polls can serve a useful purpose after Election Day in providing data on the composition and preferences of the electorate, they lack credibility in projecting election results, and they reflect poorly on the news organizations that release them prematurely. This ought to give news organizations sufficient reason to abandon the practice of releasing exit poll data before elections have been decided.

Government cannot prohibit news organizations from irresponsible political reporting, and efforts to legislate a delay in the announcement of projected election results are problematic. Voluntary restraint on the part of news organizations offers the best recourse. By exercising voluntary restraint, news organizations will enhance their credibility and better serve the American people by encouraging participation and public confidence in elections.

Recommendations on Media Projections of Election Results

7.2.1 News organizations should voluntarily refrain from projecting any presidential election results in any state until all of the polls have closed in the 48 contiguous states.

7.2.2 News organizations should voluntarily agree to delay the release of any exit poll data until the election has been decided.



(Carter Center Photo/Mario Tama)

8. Election Observation

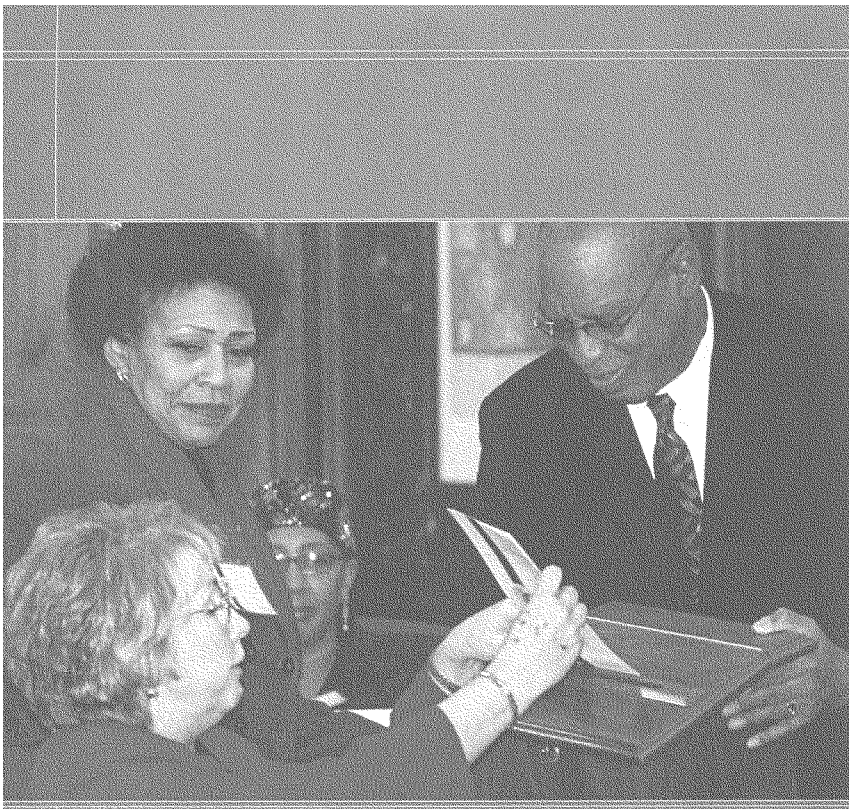
In too many states, election laws and practices do not allow independent observers to be present during crucial parts of the process, such as the testing of voting equipment or the transmission of results. In others, only certified representatives of candidates or political parties may observe. This limits transparency and public confidence in the election process. Above all, elections take place for the American people, rather than for candidates and political parties. Interested citizens, including those not affiliated with any candidate or party, should be able to observe the entire election process, although limits might be needed depending on the size of the group.

Although the United States insists on full access by its election observers to the elections of other countries, foreign observers are denied or granted only selective access to U.S. elections. Observers from the Organization for Security and Cooperation in Europe (OSCE), who were invited to the United States in 2004, were not granted access to polling stations in some states, and in other states, their access was limited to a few designated polling stations. Only one of our 50 states (Missouri) allows unfettered access to polling stations by international observers. The election laws of the other 49 states either lack any reference to international observers or fail to include international observers in the statutory categories of persons permitted to enter polling places.

To fulfill U.S. commitments to the OSCE "Copenhagen Declaration" on International Standards of Elections, accredited international observers should be given unrestricted access to U.S. elections. Such accreditation should be provided to reputable organizations which have experience in election observation and which operate in accordance with a recognized code of conduct. The National Association of Secretaries of State has encouraged state legislatures to make any necessary changes to state law to allow for international observers.[76]

Recommendation on Election Observation

8.1.1 All legitimate domestic and international election observers should be granted unrestricted access to the election process, provided that they accept election rules, do not interfere with the electoral process, and respect the secrecy of the ballot. Such observers should apply for accreditation, which should allow them to visit any polling station in any state and to view all parts of the election process, including the testing of voting equipment, the processing of absentee ballots, and the vote count. States that limit election observation only to representatives of candidates and political parties should amend their election laws to explicitly permit accreditation of independent and international election observers.



A presidential elector casts a ballot (AP Photo/Seth Perlman)

9. Presidential Primary and Post-Election Schedules

9.1 PRESIDENTIAL PRIMARY SCHEDULE

The presidential primary system is organized in a way that encourages candidates to start their campaigns too early, spend too much money, and allow as few as eight percent of the voters to choose the nominees. The Commission believes that the scheduling of the presidential primary needs to be changed to allow a wider and more deliberate national debate.

In 2000, the presidential primaries were effectively over by March 9, when John McCain ended his bid for the Republican nomination and Bill Bradley left the race for the Democratic nomination. This was less than seven weeks after the Iowa caucus. In 2004, the presidential primary process was equally compressed. Less than 8 percent of the eligible electorate in 2004 cast ballots before the presidential nomination process was effectively over.

The presidential primary schedule has become increasingly front-loaded. While 8 states held presidential primaries by the end of March in 1984, 28 states held their primaries by March in 2004. The schedule continues to tighten, as six states have moved up the date of their presidential primary to February or early March while eight states have decided to cancel their presidential primary.[77]

Because the races for the presidential nominations in recent elections have generally concluded by March, most Americans have no say in the selection of presidential nominees, and intense media and public scrutiny of candidates is limited to about 10 weeks. Moreover, candidates must launch their presidential bids many months before the official campaign begins, so that they can raise the $25 to $50 million needed to compete.

The presidential primary schedule therefore is in need of a comprehensive overhaul. A new system should aim to expand participation in the process of choosing the party nominees for president and to give voters the chance to closely evaluate the presidential candidates over a three- to four-month period. Improvements in the process of selecting presidential nominees might also aim to provide opportunities for late entrants to the presidential race and to shift some emphasis from Iowa and New Hampshire to states that more fully reflect the diversity of America.

Most members of the Commission accept that the first two states should remain Iowa and New Hampshire because they test the candidates by genuine "retail," door-to-door campaigning. A few other members of the Commission would replace those states with others that are more representative of America's diversity, and would especially recommend a change from Iowa because it chooses the candidate by a public caucus rather than a secret ballot, the prerequisite of a democratic election.

While the presidential primary schedule is best left to the political parties to decide, efforts in recent years by political parties have failed to overhaul the presidential primary schedule. If political parties do not make these changes by 2008, Congress should legislate the change.

Recommendation on Presidential Primary Schedule

9.1.1 We recommend that the Chairs and National Committees of the political parties and Congress make the presidential primary schedule more orderly and rational and allow more people to participate. We endorse the proposal of the National Association of Secretaries of State to create four regional primaries, after the Iowa caucus and the New Hampshire primary, held at one-month intervals from March to June. The regions would rotate their position on the calendar every four years.

9.2 POST-ELECTION TIMELINE

As the nation saw in 2000, a great deal of bitterness can arise when the outcome of a close presidential election turns on the interpretation of ambiguous laws. Had the U.S. Supreme Court not resolved the principal controversy in 2000, the dispute would have moved to Congress pursuant to Article II and the Twelfth Amendment. Unfortunately, the relevant provisions of the Constitution are vague or ambiguous in important respects, and the implementing legislation adopted by Congress over a century ago is not a model of clarity and consistency. If Congress is called upon to resolve a close election in the future, as could well happen, the uncertain meaning of these legal provisions is likely to lead to a venomous partisan spectacle that may make the 2000 election look tame by comparison.

After the debacle following the election of 1876, Congress spent more than a decade fashioning rules and procedures that it hoped would allow future disputes to be settled by preexisting rules. Those rules and procedures have remained on the books essentially unchanged since that time. The core provision (3 U.S.C. § 5) invites the states to establish appropriate dispute-resolution mechanisms by promising that Congress will give conclusive effect to the states' own resolution of controversies if the mechanism was established before the election and if the disputes are resolved at least six days before the electoral college meets. This "safe-harbor" provision appropriately seeks to prevent Congress itself from having to resolve election disputes involving the presidency, and every state should take steps to ensure that its election statutes qualify the state for favorable treatment under the safe-harbor provision.

Unfortunately, even if all the states take this step, disputes requiring Congress to ascertain the meaning of unclear federal rules could still arise. Although it may not be possible to eliminate all possible sources of dispute, significant steps could be taken to improve the clarity and consistency of the relevant body of federal rules, and Congress should undertake to do so before the next presidential election.

Recommendations on Post-Election Timeline

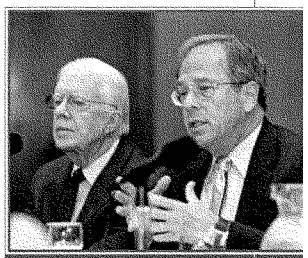
9.2.1 Congress should clarify and modernize the rules and procedures applicable to carrying out its constitutional responsibilities in counting presidential electoral votes, and should specifically examine the deadlines.

9.2.2 States should certify their presidential election results before the "safe harbor" date. Also, every state should take steps, including the enactment of new statutes if necessary, to ensure that its resolution of election disputes will be given conclusive effect by Congress under 3 U.S.C. § 5.

Conclusion

Building confidence in U.S. elections is central to our nation's democracy. The vigor of our democracy depends on an active and engaged citizenry who believe that their votes matter and are counted accurately. The reforms needed to keep our electoral system healthy are an inexpensive investment in the stability and progress of our country.

As a nation, we need to pursue the vision of a society where most Americans see their votes as both a right and a privilege, where they cast their votes in a way that leaves them proud of themselves as citizens and of democracy in the United States. Ours should be a society where registering to vote is convenient, voting is efficient and pleasant, voting machines work properly, fraud is minimized, and disputes are handled fairly and expeditiously.



Commission Co-Chair Jimmy Carter and Executive Director Robert Pastor (American University Photo/Wilford Harewood)

This report represents a comprehensive proposal for accomplishing those goals and modernizing our electoral system. We have sought to transcend partisan divides with recommendations that will both assure the integrity of the system and widen access. No doubt, there will be some who prefer some recommendations and others who prefer other proposals, but we hope that all will recognize, as we do, that the best way to improve our electoral system is to accept the validity of both sets of concerns.

The five pillars of our proposal represent an innovative and comprehensive approach. They break new ground in the following ways:

First, we propose a universal, state-based, top-down, interactive, and interoperable registration list that will, if implemented successfully, eliminate the vast majority of complaints currently leveled against the election system. States will retain control over their registration lists, but a distributed database offers a way to remove interstate duplicates and maintain an up-to-date, fully accurate registration list for the nation.

Second, we propose that all states require a valid photo ID card, which would be a slightly modified REAL ID or a photo ID that is based on an EAC-template (which is equivalent to the REAL ID without the drivers license). However, instead of allowing the ID to be a new barrier to voting, we propose using it to enfranchise new and more voters than ever before. The states would play a much more affirmative role of reaching out to the underserved communities by providing them more offices, including mobile ones, to register them and provide photo IDs free of charge. In addition, we offer procedural and institutional safeguards to make sure that the card is not abused and that voters will not be disenfranchised because of the need for an ID.

Third, we propose measures that will increase voting participation by connecting registration and the ID process, making voting more convenient, diminishing irregularities, and offering more information on voting.

Fourth, we propose ways to give confidence to voters that use the new electronic voting machines to ensure that their vote will be recorded accurately and there will be an auditable backup on paper (with the understanding that alternative technologies may be available in the future). Our proposals also aim to make sure that people with disabilities have full access to voting and the opportunity to do so privately and independently like other voters.

Finally, we recommend a restructuring of the system by which elections have been administered in our country. We propose that the Election Assistance Commission and state election management bodies be reconstituted on a nonpartisan basis to become more professional, independent, and effective.

Election reform is neither easy nor inexpensive. Nor can we succeed if we think of providing funds on a one-time basis. We need to view the administration of elections as a continuing challenge for the entire government, and one that requires the highest priority of our citizens and our government.

For more than two centuries, our country has taught the world about the significance of democracy, but more recently, we have evinced a reluctance to learn from others. Typical of this gap is that we insist other countries open their elections to international observers, but our states close their doors or set unfair restrictions on election observing. We recommend changing that provision and also building on the innovations of the new democracies by establishing new election management bodies that are independent, nonpartisan, and effective with a set of procedures that would make American democracy, once again, the model for the world.

The new electoral edifice that we recommend is built on the five pillars of reforms. Democrats, Republicans, and Independents may differ on which of these pillars are the most important, but we have come to understand that all are needed to improve our electoral system. Indeed, we believe that the structure is greater than the sum of its pillars. Substantively, the system's integrity is strengthened by the increased access of its citizens, and voter confidence is raised by accuracy and security of new technology and enforcement of election laws. And the political support necessary to implement these reforms is more likely to materialize if all the pillars are viewed as part of an entire approach. If adequately funded and implemented, this new approach will move America down the path of transforming the vision of a model democracy into reality.

APPENDIX

Estimated Costs of Recommended Improvements

The Commission's recommendations are estimated to cost $1.35 billion to implement. This estimate is the sum of the cost of making state voter databases interoperable and upgrading voting machines to make them both accessible and transparent.

The total cost for making voter databases interoperable is estimated at $287 million. This cost breaks down as follows:

- The 11 states without top-down voter registration systems will need to spend a total of $74 million to build such systems.[78]
- The system to share voter data among states is estimated to cost $77 million.[79]
- The cost for all states to adopt the recommended template for shared voter data is estimated at $21 million. Since every state except Vermont requires a Social Security number to issue a driver's license, states will need to collect Social Security numbers from only a small portion of the adult population.[80]
- Since all states currently collect digital images of signatures when they issue driver's licenses, there will be no significant cost for collecting signature images for voter registration.
- For voter identification, states that use REAL ID for voting purposes will need additional funds only to provide a template form of ID to non-drivers. The template form of ID will be issued to an estimated 23 million U.S. citizen non-drivers at a cost of $115 million.[81]

The total cost for upgrading voting machines, to make them both accessible and transparent, is estimated at $1.06 billion. This is the amount needed, in addition to the HAVA funds already obligated, to replace remaining punch card and lever machines with direct recording electronic (DRE) systems or with optical scan systems with a computer-assisted marking device for blind and visually impaired voters, to retrofit DREs with a voter-verifiable paper audit trail, and to add a ballot marking device for blind voters to existing optical scan systems. The estimates are based on current distributions of various voting machines and on current costs for DREs, voter-verifiable paper audit trails, and ballot-marking devices for optical scan systems.

The Commission recommends that Congress provide $1.35 billion in funding over a two-year period, so that voter databases will be made interoperable and voting machine upgrades will be completed before the 2008 elections.

ENDNOTES

[1] Adam Nagourney and Janet Elder, "Late Poll Still Shows Sharp Split in U.S. Vote," *International Herald Tribune,* November 1, 2004; and Dan Eggen, "Justice Department Triples Election Monitors: More than 1,000 Head to Polls," *The Washington Post,* October 29, 2004, p. A6.

[2] The Pew Research Center for the People and the Press, "Voters Liked Campaign 2004, But Too Much 'Mud-Slinging'," November 11, 2004, available at <http://people-press.org/reports/display.php3?ReportID=233>.

[3] Milwaukee Police Department, Milwaukee County District Attorney's Office, Federal Bureau of Investigation, and United States Attorney's Office Task Force, *Preliminary Findings of Joint Task Force Investigating Possible Election Fraud.* May 10, 2005. Available at <http://www.wispolitics.com/1006/electionfraud.pdf>.

[4] "Dead voters on rolls," *Chicago Tribune,* December 4, 2004.

[5] The following democracies constitute some of the nearly 100 countries that utilize a national ID system: Belgium, Cost Rica, Germany, India, Italy, the Netherlands, Portugal, South Africa, and Spain. See Privacy.org, "Identity Cards: FAQ," August 24, 1996, available at <http://www.privacy.org/pi/activities/idcard/idcard_faq.html>

[6] Jason P. Schacter, "Geographical Mobility: 2002 to 2003." *Current Population Reports.* US Census Bureau (March 2004). Available at: http://www.census.gov/prod/2004pubs/p20-549.pdf.

[7] In addition to the 38 states with top-down voter registration systems, 6 states are developing bottom-up systems, 2 will use systems with both top-down and bottom-up elements, and 3 have yet to finalize their plans. North Dakota does not require voter registration. See Electionline.org, *Assorted Rolls: Statewide Voter Registration Databases Under HAVA,* June 2005, p. 3, available at <www.electionline.org/Portals/1/Assorted percent20Rolls.pdf>.

[8] "Exposed: Scandal of double voters," *New York Daily News,* August 21, 2004 and "Double votes taint Florida, records show," *Orlando Sentinel,* October 23, 2004.

[9] "Report: As many as 60,000 people file to vote in both Carolinas," Associated Press, October 24, 2004.

[10] "Exposed: Scandal of Double Voters," *New York Daily News,* August 21, 2004.

[11] The introduction of electronic transaction standards would also facilitate cross-state exchanges of voter data, see R. Michael Alvarez and Thad E. Hall, "The Next Big Election Challenge: Developing Electronic Data Transaction Standards for Election Administration," Caltech/MIT Voting Technology Project, July 2005, pp. 19-21.

[12] "Overview of States Driver's License Requirements", National Immigration Law Center, July 12, 2005, available at <www.nilc.org/immspbs/DLs/state_dl_rqrmts_ovrvw_071205.pdf>. Alabama also collects Social Security numbers for driver's licenses, according to Commission staff conversation with Alabama's Motor Vehicle Division in August 2005.

[13] Except for Vermont, all states require a Social Security Number for a driver's license, at least from people who were assigned a Social Security Number or are eligible for one.

[14] Voters should also have the opportunity to check their registration over the phone, via a toll-free number, or in person at the elections office.

[15] Electionline.org, *Solution or Problem? Provisional Ballots in 2004*, April 2005, p. 2, available at <http://electiononline.org/Portals/1/Publications/ERIP10Apr05.pdf>.

[16] Ibid, p.5.

[17] In states with unified databases, provisional ballots constituted .85 percent of the total ballots cast whereas in the states without unified databases, provisional ballots constituted 1.76 percent of the total. See Electionline.org, *Solution or Problem? Provisional Ballots in 2004*, Washington, D.C., April 2005.

[18] Testimony before the Commission by Ken Smukler, President of Info Voter Technologies, on June 30, 2005.

[19] Details were provided in Section 1.1.

[20] ID is required of all voters in 22 states and of all first-time voters in another two states, according to Electionline.org, <http://electionline.org/Default.aspx?tabid=364>.

[21] Provided by Electionline.org, <www.electionline.org/Default.aspx?tabid=473>.

[22] A comparison of driver's license records and census data for 2003 suggests that about 88 percent of Americans aged 18 and over have a driver's license, see U.S. Department of Transportation, Federal Highway Administration, *Licensed Total Drivers, By Age, 2003*, Table DL-22, Oct. 2004, at <www.fhwa.dot.gov/policy/ohim/hs03/htm/dl22.htm>, and U.S. Census Bureau, *Annual Estimates of the Population by Selected Age Groups and Sex for the United States: April 1, 2000 to July 1, 2004*, (June 2005), available at <www.census.gov/popest/national/asrh/NC-EST2004-sa.html>.

[23] U.S. Government Accountability Office, *Elections: Additional Data Could Help State and Local Elections Officials Maintain Accurate Voter Registration Lists*, GAO-05-478, June 2005, pp. 13-29.

[24] U.S. Election Assistance Commission, *The Impact of the National Voter Registration Act, 2003-2004*, June 30, 2005, pp. 16 and 20.

[25] Data on voter registration in Alaska is contained in U.S. Election Assistance Commission, "The Impact of the National Voter Registration Act of 1993 on the Administration of Elections for Federal Office: 2003-2004," Table 1: Registration History. Other examples include 34 of the 82 counties in Mississippi and the City of East St. Louis, see Emily W. Pettus, "Secretary of state seeks proposals on statewide voter roll," *Associated Press*, September 1, 2004, and Mike Fitzgerald, "Dual registration: a recipe for fraud?" *Belleview News-Democrat*, November 28, 2004.

[26] For example, see Australian National Audit Office, *Integrity of the Electoral Roll*, April 2002: <www.anao.gov.au/WebSite.nsf/Publications/4A256AE90015F69BCA256B9E007B5F52>. This audit estimated that Australia's electoral rolls were 96 percent accurate, 95 percent complete, and 99 percent valid.

[27] The residual vote rates fell by 0.79 percent in counties where lever machines were replaced by direct recording electronic (DRE) machines and by 1.46 percent in counties where punch cards were replaced by DREs, according to Charles Stewart, *Residual Vote in the 2004 Election*, Caltech/MIT Voting Technology Project Working Paper, February 2005, Table 2.

[28] Election Data Services, <www.electiondataservices.com/VotingSummary2004_20040805.pdf>.

[29] Dan Keating, "Lost Votes in N.M. a Cautionary Tale," *Washington Post*, August 22, 2004, and "Nearly 40 votes may have been lost in Palm Beach County," *Associated Press*, November 2, 2004.

[30] Electionline.org, <http://www.electionline.org/Default.aspx?tabid=290>.

[31] Ted Selker, "Processes Can Improve Electronic Voting," Caltech/MIT Voting Technology Project, October 2004, available at <http://www.vote.caltech.edu/media/documents/vtp_wp17.pdf>.

[32] Manual audits of voting machines are required in Colorado, Connecticut, Hawaii, Illinois, Minnesota, New Mexico, New York, North Carolina, Washington, and West Virginia, according to Verified Voting Foundation, "Manual Audit Requirement," August 18, 2005, available at <www.verifiedvoting.org/downloads/Manual_Audit_Provisions.pdf>.

[33] Ted Selker and Jon Goler, "Security Vulnerabilities and Problems with VVPT," Caltech/MIT Voting Technology Project, April 2004, available at <http://vote.caltech.edu/media/documents/wps/vtp_wp16.pdf>.

[34] "Voting Machine Fails Inspection," *CNETNews.com*, July 23, 2003 and "New Security Woes for E-Vote Firm," *WiredNews.com*, August 7, 2003.

[35] In California's field test, about one in ten machines malfunctioned, see "Voting Machines Touch and Go," *Associated Press*, July 30, 2005.

[36] Internet Policy Institute, *Report of the National Workshop on Internet Voting: Issues and Research Agenda*, March 2001. Available at <http://news.findlaw.com/hdocs/docs/election2000/nsfe-voterprt.pdf>.

[37] Curtis Gans, "Making it Easier Doesn't Work: No Excuse Absentee and Early Voting Hurt Voter Turnout," Center for the Study of the American Electorate, September 13, 2004, available at <http://www.american.edu/ia/cfer/research/csae_09132004.pdf >.

[38] Testimony before the Commission by Robert Stein, Dean of Social Sciences at Rice University, on June 30, 2005.

[39] *Balancing Access and Integrity: The Report of the Century Foundation working Group on State Implementation of Election Reform* (N.Y. the Century Foundation Press, 2005), pp. 25-26.

[40] Curtis Gans, "Making it Easier Doesn't Work: No Excuse Absentee and Early Voting Hurt Voter Turnout," Center for the Study of the American Electorate, September 13, 2004, available at <http://www.american.edu/ia/cfer/research/csae_09132004.pdf >.

[41] Superior Court of the State of Washington for Chelan County, Final Judgment Dismissing Election Contest with Prejudice and Confirming Certification of Election of Christine Gregoire, Court Decision No. 05-2-00027-3, June 6, 2005.

[42] United States General Accounting Office. "Elections: Issues Affecting Military and Overseas Absentee Voters," May 2001, available at: <http://www.gao.gov/new.items/d01704t.pdf>, p.1.

[43] National Defense Committee, *Military and Overseas Absentee Voting in the 2004 Presidential Election*, March 30, 2005, available at <www.nationaldefensecommittee.org/media/pdf/NDCmavexecsumfinal-33005.pdf>.

[44] David Jefferson, Aviel D. Rubin, Barbara Simons, and David Wagner, *A Security Analysis of the Secure Electronic Registration and Voting Experiment*, January 20, 2004, <www.servesecutityreport.org/>.

[45] Information provided to the Commission by the Federal Voting Assistance Program.

[46] Testimony before the Commission by James Dickson, Vice President at the American Association of People with Disabilities, on April 18, 2005.

[47] Ibid.

[48] Ibid.

[49] Ibid.

[50] Alabama, Arizona, Delaware, Maryland, Mississippi, Nebraska, Nevada, Tennessee, Washington, and Wyoming have a permanent ban on voting by certain categories of ex-felons, according to the Sentencing Project, <www.sentencingproject.org/pdfs/1046.pdf>.

[51] Census data provided by the Center for Information and Research on Civic Learning and Engagement (CIRCLE), available at <www.civicyouth.org/PopUps/ReleaseCPS04_Youth.pdf>.

[52] Karl T. Kurtz, Alan Rosenthal, and Cliff Zukin, *Citizenship: A Challenge for All Generations*, National Conference of State Legislatures, September 2003, available at <www.ncsl.org/public/trust/citizenship.pdf>.

[53] Campaign for the Civic Mission of Schools and Alliance for Representative Democracy, "From Classroom to Citizen: American Attitudes on Civic Education," December 2004, available at <www.representativedemocracy.org/CivicEdSurveyReport.pdf>.

[54] U.S. Department of Justice press release, "Department of Justice to Hold Ballot Access and Voting Integrity Symposium," August 2, 2005.

[55] U.S. Government Accountability Office, *Elections: Additional Data Could Help State and Local Elections Officials Maintain Accurate Voter Registration Lists*, GAO-05-478, June 2005, pp. 59-60.

[56] *Balancing Access and Integrity: The Report of the Century Foundation working Group on State Implementation of Election Reform* (N.Y. the Century Foundation Press, 2005), pp. 67-69.

[57] John Fund, *Stealing Elections: How Voter Fraud Threatens Our Democracy* (San Francisco: Encounter Books, 2004), p. 103.

[58] Joe Stinebaker, "Loophole lets foreigners illegally vote," *Houston Chronicle*, January 16, 2005, and Robert Redding, "Purging illegal aliens from voter rolls not easy: Maryland thwarted in tries so far," *Washington Times*, August 23, 2004.

[59] Susan Greene and Karen E. Crummy, "Vote Fraud Probed In State," *Denver Post*, March 24, 2005; Brendan Farrington, "Fla. Officials Asked To Probe Vote Fraud," *Associated Press*, October 7, 2004; Dawson Bell, "Campaign Workers Suspected Of Fraud," *Detroit Free Press*, September 23, 2004; "Man Pleads Guilty In Voter Registration Scam," *Associated Press*, December 7, 2004; Robert Patrick, "Jury Finds Montgomery Guilty In Vote Fraud Case," *St. Louis Post-Dispatch*, February 11, 2005; Nevada Secretary Of State, "Alleged Vote Fraud Investigations Ongoing," Press Release, October 28, 2004; Dan McKay, "Election 'Mischief' Under Scrutiny," *Albuquerque Journal*, September 10, 2004; "Voter Registration Investigation One Of Largest In Recent Years," *Associated Press*, September 23, 2004; Greg

J. Borowski, "Inquiry Finds Evidence Of Fraud In Election," *Milwaukee Journal Sentinel*, May 11, 2005; U.S. Department of Justice, Criminal Division, Public Integrity Section, *Election Fraud Prosecutions and Convictions: Ballot Access & Voting Integrity Initiative,* October 2002 - July, 2005.

[60] A Rasmussen Reports poll just before the November 2004 elections showed that 58 percent of American voters believed there was "a lot" or "some" fraud in U.S. elections, and in a post-election NBC News/*Wall Street Journal* poll, more than a quarter of Americans worried that the vote count for president in 2004 was unfair, quoted in Rick Hasen, "Beyond the Margin of Litigation: Reforming Election Administration to Avoid Electoral Meltdown," Paper prepared for American Political Science Association meeting, September 1, 2005, pp. 7-8, available at <http://convention2.allacademic.com/getfile.php?file=apsa05_proceeding/2005-07-29/41404/apsa05_proceeding_41404.pdf&PHPSESSID=c47830ae1716d461356f998599faea17 >.

[61] Ibid, p. 9.

[62] Ibid, p. 29.

[63] International IDEA, Code of Conduct for the Ethical and Professional Administration of Elections, 1997, <www.idea.int/publications/conduct_admin/upload/adm_english.pdf>.

[64] United States Election Assistance Commission, *Background on the Help America Vote College Poll Worker Program.* <http://www.eac.gov/coll_poll_background.asp>; Associated Press, "US short of poll workers" November 1, 2004, *Fox News.* Available at: <http://www.foxnews.com/story/0,2933,137242,00.html>

[65] The Voting Rights Institute, *Democracy at Risk: the 2004 Election in Ohio* (Washington, D.C.: Democratic National Committee, 2005).

[66] U.S. Department of Justice's investigations in Franklin County and in Knox County, Ohio found no evidence that the allocation of voting machines was conducted in a discriminatory manner, see <www.usdoj.gov/crt/voting/misc/franklin_oh.htm> and <www.usdoj.gov/crt/voting/misc/knox.htm>. In fact, the distribution of voting machines was determined by each county's Board of Elections, and half the members of each Board of Elections are Democrats.

[67] Rule §81.125 of Texas Administrative Code, available at <http://info.sos.state.tx.us/pls/pub/readtac$ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=1&pt=4&ch=81&rl=125>.

[68] A strong example of funding for elections research is the $7.5 million awarded by the National Science Foundation on August 15, 2005 for a collaborative project of six institutions to study the reliability, security, transparency, and auditability of voting systems.

[69] California Secretary of State *Historical Close Of Registration Statistics: Presidential General Elections,* May 2004, available at <www.ss.ca.gov/elections/ror/reg_stats_10_18_04.pdf>; Wyoming Secretary of State, *Profile of Wyoming's Voters: Voter Registration and Voter Turnout, Associated Press,* 2004. Available at <soswy.state.wy.us/election/profile.htm>. *Election cost — $4 billion and climbing: most money went for ads, but other expenses not chicken feed.* Available at <www.msnbc.msn.com/id/6388580/>.

[70] IFES, Cost of Registration and Elections (CORE) for election costs in Australia and Spain; Elections Canada, <www.elections.ca/>; Electionguide.org, <www.electionguide.org/resultsum/canada_par04.htm>; UK Electoral Commission, 2002, *Funding Democracy: Providing Cost-Effective Electoral Services*, available at <www.electoralcommission.org.uk/files/dms/funding_csltppr_6642-6213__E__N__S__W__.pdf>; Electionguide.org, EPIC Project, available at <epicproject.org/ace/compepic/en/getAnswer$ALL+EM10>.

[71] Alliance for Better Campaigns, <www.bettercampaigns.org/standard/display.php?StoryID=322>.

[72] Fox New/Opinion Dynamics poll, March 25, 2004, <www.foxnews.com/story/0,2933,115208,00.html>.

[73] Analysis by the Norman Lear Center at the Annenberg School for Communication of the University of Southern California, <www.bettercampaigns.org/standard/display.php?StoryID=328>.

[74] Alliance for Better Campaigns, <www.bettercampaigns.org/standard/display.php?StoryID=326>, and Lear Center, "Local News Coverage of the 2004 Campaigns."

[75] National Commission on Federal Election Reform, *To Assure Pride and Confidence in the Electoral Process*, August 2001, p. 63.

[76] National Association of Secretaries of State, "International Election Protocol Resolution," and supporting language, July 24, 2005, available at <www.nass.org/International Election Protocol Resolution.pdf> and <www.nass.org/International Elections Protocol Language.pdf>.

[77] Six states passed measures to move forward the date of their presidential primaries and eight states passed measures to cancel their presidential primary for 2004, see <www.ncsl.org/programs/legman/elect/taskfc/Changing-EliminatingPP.htm>.

[78] Estimate is based on the average amounts other states are currently spending to build top-down voter registration systems and excludes HAVA funds that have already been disbursed for this purpose see Electiononline.org, *Assorted Rolls: Statewide Voter Registration Databases Under HAVA*, <http://electionline.org/Portals/1/Assorted Rolls.pdf>.

[79] Figure includes both the cost to upgrade existing state databases to make them interoperable in real time and the cost to build a voter registration distributed database linked to the individual state servers. The former ($48 million) is based on the average cost to make existing state driver's license databases interoperable with each other as determined by the Congressional Budget Office, see "H.R. 418: REAL ID Act of 2005," Congressional Budget Office, <http://www.cbo.gov/showdoc.cfm?index=6072&sequence=0>. The latter ($29 million) is based on the market cost to purchase, secure, maintain, and link to the states through leased lines a central database that benchmarks 57,346 transactions per minute.

[80] The cost to collect Social Security numbers is tantamount to registering voters. The Office of the Chief Electoral Officer of Canada calculates the cost to registering 19.6 million voters in the 1997 national elections at approximately $18 million. This produces a statistic of $0.92 to register each person, see *Voter Turnout*, electionguide.org, <http://www.electionguide.org/turnout.htm> and *Voting for Democracy: Notes on the Canadian Experience*, Office of the Chief Electoral Officer of Canada, March 1998, <http://www.aceproject.org/main/samples/vr/vrx_w005.pdf>. For data on the distribution of driver's licenses, see "Highway Statistics 2003," U.S. Department of Transportation, <http://www.fhwa.dot.gov/policy/ohim/hs03/htm/dl22.htm>.

[81] The cost per card is estimated at $5. This figure includes approximate administrative, infrastructure, and issuance costs, see Stephen Moore, "Congressional testimony before the U.S. House of Representatives Subcommittee on Immigration and Claims, Judiciary Committee," May 13, 1997, available at <http://www.cato.org/testimony/ct-sm051397.html> and "The debate over a national identification card," The Century Foundation, Homeland Security Project, available at <http://www.tcf.org/Publications/HomelandSecurity/National_ID_Card.pdf>.

[82] The estimated costs for the various voting machines are as follows: Direct Recording Electronic with a Voter-Verified Paper Audit Trail (DRE/VVPAT)—$4,000; retrofitting a DRE machine with a VVPAT—$1,000; optical scanner (OS)—$5,000; and ballot marking device for an optical scan system—$4,500. Machine cost data is collected from many sources, including: Verifiedvoting.org, "Appendix 4: Cost Comparison of Alternative Solutions," <http://www.verifiedvoting.org/downloads/CT SOTS1appendix_43.pdf>; Caleb Kleppner, *State of the Industry: Compatibility of Voting Equipment with Ranked Ballots*, Center for Voting and Democracy, 2001, <http://www.fairvote.org/administration/industry.rtf>; Bo Lipari, "Analysis of Acquisition Costs of DRE and Precinct Based Optical Scan Voting Equipment for New York State," New Yorkers for Verified Voting, 2005, <http://www.nyvv.org/doc/AcquisitionCostDREvOptScanNYS.pdf>. For details on the distribution of machine technology, see Election Data Services, *Voting Equipment Summary by Type*, 2004, <http://www.electiondataservices.com/VotingSummary2004_20040805.pdf>.

THE MACHINERY OF DEMOCRACY: PROTECTING ELECTIONS IN AN ELECTRONIC WORLD

BRENNAN CENTER TASK FORCE
ON VOTING SYSTEM SECURITY,
LAWRENCE NORDEN, CHAIR



VOTING RIGHTS
& ELECTIONS SERIES

BRENNAN CENTER
FOR JUSTICE
AT NYU SCHOOL OF LAW

THE MACHINERY OF DEMOCRACY: PROTECTING ELECTIONS IN AN ELECTRONIC WORLD

THE BRENNAN CENTER TASK FORCE
ON VOTING SYSTEM SECURITY
LAWRENCE NORDEN, CHAIR

VOTING RIGHTS
& ELECTIONS SERIES

BRENNAN CENTER
FOR JUSTICE
AT NYU SCHOOL OF LAW
www.brennancenter.org

ABOUT THE TASK FORCE

In 2005, the Brennan Center convened a Task Force of internationally renowned government, academic, and private-sector scientists, voting machine experts and security professionals to conduct the nation's first systematic analysis of security vulnerabilities in the three most commonly purchased electronic voting systems. The Task Force spent more than a year conducting its analysis and drafting this report. During this time, the methodology, analysis, and text were extensively peer reviewed by the National Institute of Standards and Technology ("NIST"). The members of the Task Force are:

Chair
Lawrence D. Norden, Brennan Center for Justice

Principal Investigator
Eric L. Lazarus, DecisionSmith.

Experts
Georgette Asherman, independent statistical consultant, founder of Direct Effects

Professor Matt Bishop, University of California at Davis

Lillie Coney, Electronic Privacy Information Center

Professor David Dill, Stanford University

Jeremy Epstein, PhD, Cyber Defense Agency LLC

Harri Hursti, independent consultant, former CEO of F-Secure PLC

Dr. David Jefferson, Lawrence Livermore National Laboratory and Chair of the California Secretary of State's Voting Systems Technology Assessment and Advisory Board

Professor Douglas W. Jones, University of Iowa

John Kelsey, PhD, NIST

Rene Peralta, PhD, NIST

Professor Ronald Rivest, MIT

Howard A. Schmidt, Former Chief Security Officer, Microsoft and eBay

Dr. Bruce Schneier, Counterpane Internet Security

Joshua Tauber, PhD, formerly of the Computer Science and Artificial Intelligence Laboratory at MIT

Professor David Wagner, University of California at Berkeley

Professor Dan Wallach, Rice University

Matthew Zimmerman, Electronic Frontier Foundation

© 2006. This paper is covered by the Creative Commons "Attribution-No Derivs-NonCommercial" license (see http://creativecommons.org). It may be reproduced in its entirety as long as the Brennan Center for Justice at NYU School of Law is credited, a link to the Center's web page is provided, and no charge is imposed. The paper may not be reproduced in part or in altered form, or if a fee is charged, without the Center's permission. Please let the Center know if you reprint.

ABOUT THE EDITOR AND TASK FORCE CHAIR

Lawrence Norden is an Associate Counsel with the Brennan Center, working in the areas of voting technology, voting rights, and government accountability. For the past year, Mr. Norden has led the Brennan Center's voting technology assessment project. He is the lead author of *The Machinery of Democracy: Voting System Security, Accessibility, Usability, Cost* (Brennan Center forthcoming 2006) and a contributor to Routledge's forthcoming *Encyclopedia of American Civil Liberties.* Mr. Norden edits and writes for the Brennan Center's blog on New York State, www.ReformNY.blogspot.com. He is a graduate of the University of Chicago and the NYU School of Law. Mr. Norden serves as an adjunct faculty member in the Lawyering Program at the Benjamin N. Cardozo School of Law. He may be reached at lawrence.norden@nyu.edu.

ABOUT THE BRENNAN CENTER

The Brennan Center for Justice at NYU School of Law unites thinkers and advocates in pursuit of a vision of inclusive and effective democracy. The organization's mission is to develop and implement an innovative, nonpartisan agenda of scholarship, public education, and legal action that promotes equality and human dignity, while safeguarding fundamental freedoms. The Center works in the areas of Democracy, Poverty, Criminal Justice, and Liberty and National Security. Michael Waldman is the Center's Executive Director.

ABOUT THE VOTING RIGHTS & ELECTIONS SERIES

The Brennan Center's Voting Rights & Elections Project promotes policies that protect rights to equal electoral access and political participation. The Project seeks to make it as simple and burden-free as possible for every eligible American to exercise the right to vote and to ensure that the vote of every qualified voter is recorded and counted accurately. In keeping with the Center's mission, the Project offers public education resources for advocates, state and federal public officials, scholars, and journalists who are concerned about fair and open elections. For more information, please see www.brennancenter.org or call 212-998-6730.

This paper is the second in a series, which also includes:

Making the List: Database Matching and Verification Processes for Voter Registration by Justin Levitt, Wendy Weiser and Ana Muñoz.

Other resources on voting rights and elections, available on the Brennan Center's website, include:

Response to the Report of the 2005 Commission on Federal Election Reform (2005) (co-authored with Professor Spencer Overton)

Recommendations for Improving Reliability of Direct Recording Electronic Voting Systems (2004) (co-authored with Leadership Conference on Civil Rights)

ACKNOWLEDGMENTS

Most importantly, the Brennan Center thanks NIST and its many scientists for devoting so many hours to its extensive and thorough peer review of the analysis and report. The report, in its current form, would not exist without NIST's many important comments and contributions.

In particular, we thank John Kelsey of NIST for the substantial material and ideas he provided, which have been incorporated into the report and the report's attack catalogs. We also specially thank Rene Peralta for his original contributions and analysis. Finally, we are enormously grateful to Barbara Guttman, John Wack and other scientists at NIST, who provided material for the attack catalogs, helped to develop the structure of the report, and edited many drafts.

We are also extremely appreciative of Principal Investigator Eric Lazarus's enormous efforts on behalf of this report. His vision, tenacity, and infectious enthusiasm carried the team through a lengthy process of analysis and drafting.

A special debt of gratitude is also owed to election officials throughout the country, who spent many hours responding to surveys and interview questions related to this report. In addition to team members Professor Ronald Rivest and Dr. David Jefferson, we particularly thank Patrick Gill, Woodbury County Auditor and Recorder and Past President of the Iowa State Association of County Auditors; Elaine Johnston, County Auditor, Asotin County, Washington; Harvard L. Lomax, Registrar of Voters for Clark County, Nevada; Debbie Smith, Elections Coordinator, Caleveras County, California; Jocelyn Whitney, Developer and Project Manager for parallel testing activities in the State of California; Robert Williams, Chief Information Officer for Monmouth County, New Jersey; and Pam Woodside, former Chief Information Officer for the Maryland State Board of Elections. We would also like to acknowledge the National Committee for Voting Integrity for their cooperation and assistance in this effort.

Jeremy Creelan, Associate Attorney at Jenner & Block LLP, deserves credit for conceiving, launching, and supervising the Brennan Center's voting technology assessment project, including development of this report, as Deputy Director of the Center's Democracy Program through February 2005. The Program misses him greatly and wishes him well in private practice, where he continues to provide invaluable *pro bono* assistance.

The Brennan Center is grateful to Task Force member Lillie Coney, Associate Director of the Electronic Privacy Information Center. Among many other contributions, she provided invaluable assistance in assembling the Task Force, and frequently offered the Brennan Center sage strategic advice.

This report also benefited greatly from the insightful and thorough editorial assistance of Deborah Goldberg, Director of the Brennan Center's Democracy

Program. We are extremely grateful to Professor Henry Brady of the University of California at Berkeley and Professor Benjamin Highton of the University of California at Davis for their insights into the possible effects of denial-of-service attacks on voting systems. The Brennan Center also thanks Bonnie Blader, independent consultant, who provided the Task Force with crucial research, David M. Siegel, independent technology consultant, for his original contributions on the subject of software code inspections, and Tracey Lall, Ph.D. candidate in Computer Science at Rutgers University, who contributed many hours of critical security analysis. Douglas E. Dormer, CPA, CTP provided invaluable assistance in developing the analysis methodology and in keeping the task force focused. Joseph Lorenzo Hall also must be thanked for helping the Task Force members understand the diversity and commonality in voting system architectures. Much of the legal research was conducted by Gloria Garcia and Juan Martinez, J.D. candidates at Benjamin N. Cardozo School of Law, and Annie Lai and S. Michael Oliver, J.D. candidates at NYU School of Law. Lowell Bruce McCulley, CSSP, was exceptionally helpful in creating the attack catalogs. Finally, we thank Brennan Center Research Associates Annie Chen, Lauren Jones, Ana Muñoz, and Neema Trivedi for their many hours of dedicated assistance.

Generous grants from an anonymous donor, the Carnegie Corporation of New York, the Ford Foundation, the HKH Foundation, the Knight Foundation, the Open Society Institute, and the Rockefeller Family Fund supported the development and publication of this report. The statements made and views expressed in this report are the responsibility solely of the Brennan Center.

CONTENTS

Introduction 1
Limitations of Study 1
Summary of Findings and Recommendations 3

The Need for a Methodical Threat Analysis 6
Recurrent, Systematic Threat Analyses of Voting Systems Are Long Overdue 6
Solid Threat Analyses Should Help Make Voting Systems More Reliable 6

Methodology 8
Identification of Threats 8
Prioritizing Threats: Number of Informed Participants as Metric 8
Determining Number of Informed Participants 10
Determining the Steps and Values for Each Attack 10
Number of Informed Participants Needed to Change Statewide Election 11
Limits of Informed Participants as Metric 12
Effects of Implementing Countermeasure Sets 13
Countermeasures Examined 14
Basic Set of Countermeasures 14
Inspection 14
Physical Security for Machines 14
Chain of Custody/Physical Security of Election Day Records 15
Testing 15
Regimen for Automatic Routine Audit Plus Basic Set of Countermeasures 16
The Audit 16
Transparent Random Selection Process 17
Regimen for Parallel Testing Plus Basic Set of Countermeasures 18
Parallel Testing 18
Transparent Random Selection Process 19

Representative Model for Evaluation of Attacks and Countermeasures: Governor's Race, State of Pennasota, 2007 20
Facts About Pennasota 20
Evaluating Attacks in Pennasota 20
Limits on Attacker 22
Targeting the Fewest Counties 23
Testing the Robustness of Our Findings 23

The Catalogs 24
Nine Categories of Attacks 24
Lessons from the Catalogs: Retail Attacks Should Not Change the Outcome of Most Close Statewide Elections 27

Software Attacks on Voting Machines 30
History of Software-Based Attacks 30
Vendor Desire to Prevent Software Attack Programs 32
Inserting the Attack Program 33
Points of Attack: COTS and Vendor Software 33
Points of Attack: Software Patches and Updates 35
Points of Attack: Configuration Files and Election Definitions 35
Points of Attack: Network Communication 36
Points of Attack: Device Input/Output 36
Technical Knowledge 36
Election Knowledge 37
Attacking the Top of the Ticket 37
Parameterization 38
Creating an Attack Program That Changes Votes 39
Changing System Settings or Configuration Files 39
Active Tampering with User Interaction or Recording of Votes 40
Tampering with Electronic Memory After the Fact 40
Eluding Independent Testing Authority Inspections 42
Create Different Human-Readable and Binary Code 42
Use Attack Compiler, Linker, Loader or Firmware 42
Avoiding Inspection Altogether 43
Avoiding Detection During Testing 44
Avoiding Detection After the Polls Have Closed 44
Deciding How Many Votes to Change 45
Avoiding Event and Audit Logs 45
Coordinating with Paper Record Attacks 46
Conclusions 47

Least Difficult Attacks Applied Against Each System 48
Attacks Against DREs Without VVPT 48
Representative "Least Difficult" Attack: Trojan Horse Inserted Into Operating System (DRE Attack Number 4) 49
Description of Potential Attack 49
How the Attack Could Swing Statewide Election 50
Effect of Basic Set of Countermeasures 51
Effect of Regimen for Parallel Testing 52
Infiltrating the Parallel Testing Teams 53
Creating an Attack That Recognizes Testing 53
Warning the Trojan Horse 54

Detecting the Test Environment 56
Recognizing Voting Patterns 57
Recognizing Usage Patterns 58
Taking Action When Parallel Testing Finds Discrepancies .. 59
Conclusions and Observations 59
Attacks Against DREs w/VVPT 61
Representative "Least Difficult" Attack: Trojan Horse Triggered with Hidden Commands in Ballot Definition File (DRE w/VVPT Attack Number 1a) 62
Attacking Both Paper and Electronic Records (DRE w/VVPT Attack Number 6) 65
Paper Misrecords Vote 65
Do Voters Review VVPT? 66
Effect of Regimen for Parallel Testing Plus Basic Set of Countermeasures 68
Effect of Regimen for Automatic Routine Audit Plus Basic Set of Countermeasures 68
Trojan Horse Attacks Paper at Time of Voting, Voters Fail to Review 69
Co-opting the Auditors 71
Replacing Paper Before the Automatic Routine Audit Takes Place 71
Replacing Some Paper Records Merely to Add Votes 73
Taking Action When Automatic Routine Audit Finds Anomalies 74
Conclusions 75
Attacks Against PCOS 77
Representative "Least Difficult" Attack: Software Attack Inserted on Memory Cards (PCOS Attack Number 41) 78
Description of Attack 78
Effect of Basic Set of Countermeasures 80
Effect of Regimen for Parallel Testing Plus Basic Set of Countermeasures 80
Effect of Regimen for Automatic Routine Audit Plus Basic Set of Countermeasures 81
PCOS Attack Number 42: Trojan Horse Disables Overvote Protections 81
PCOS Attack Number 49: Attack on Scanner Configuration Causes Misrecording of Votes 82
Conclusions 83

Prevention of Wireless Communication: A Powerful Countermeasure for All Three Systems 85

Security Recommendations 87

Directions for the Future 92
Witness and Cryptographic Systems 92
Informing Voters of Their Role in Making Systems More Secure 92
Additional Statistical Technical Techniques to Detect Fraud 92
Looking for Better Parallel Testing Techniques 93
Looking at Other Attack Goals 93
Looking at Other Races 93

Glossary 94

Endnotes 96

Appendices
Appendix A. Alternative Threat Analysis Models Considered 112
Appendix B. Voting Machine Definitions 114
Appendix C. Alternative Security Metrics Considered 115
Appendix D. Brennan Center Security Survey 116
Appendix E. Voting Machine Testing 119
Appendix F. Example of Transparent Random Selection Processes ...127
Appendix G. Assumptions 129
Appendix H. Tables Supporting Pennasota Assumptions 132
Appendix I. Denial-of-Service Attacks 136
Appendix J. Chances of Catching Attack Program Through Parallel Testing 139
Appendix K. Chances of Catching Attack Program Through the ARA .142
Appendix L. Subverting the Audit 143
Appendix M. Effective Procedures for Dealing With Evidence of Fraud or Error 147

Figures
Figure 1. Voting Systems 2
Figure 2. Election for Governor, State of Pennasota, 2007. 20
Figure 3. Assumed Precautions Taken by Attacker: Limits on the % of Votes Added or Subtracted for a Candidate. 22
Figure 4. Total Votes Johnny Adams Needs to Switch to Ensure Victory: 51,891 23
Figure 5. Typical Flow of Information To and From Voting Machines . .24
Figure 6. Software Attack Program: Points of Entry 34
Figure 7. Possible Attack on DRE with VVPT 64
Figure 8. Where 3% of Voters Check VVPT 66
Figure 9. Where 20% of Voters Check VVPT 67

INTRODUCTION

This analysis should assist jurisdictions decide which voting systems to certify or purchase, and how to protect those systems from security threats after they have been purchased.

Problems with voting system security are making headlines like never before. The issue is attracting attention because of a number of factors: the rash of close, high-profile elections since 2000, greater attention to security since September 11, 2001, the recent shift in many states from mechanical to computerized voting systems, and high-profile reports about hacking of common electronic voting machines.

Public attention to voting system security has the potential to be a positive force. Unfortunately, too much of the public discussion surrounding security has been marred by claims and counter-claims that are based on little more than speculation or anecdote.

In response to this uninformed discussion, and with the intention of assisting election officials and the public as they make decisions about their voting machines, the Brennan Center for Justice at NYU School of Law assembled a Task Force of internationally renowned government, academic and private-sector scientists, voting machine experts, and security professionals to perform a methodical threat analysis of the voting systems most commonly purchased today. This is, as far as we know, the first systematic threat analysis of these voting systems. The methodology, analysis, and text were extensively peer reviewed by the National Institute of Standards and Technology ("NIST").

In this report, the Task Force reviews several categories of threats to the technologies of three electronic voting systems. Direct Recording Electronic voting systems ("DREs"), DREs with a voter-verified auditable paper trail ("DREs w/VVPT") and Precinct Count Optical Scan ("PCOS") systems. We then identify, as against each system, the least difficult way for an attacker to change the outcome of a statewide election. And finally, we examine how much more difficult different sets of countermeasures would make these least difficult attacks. We believe that this analysis, together with the concurrent findings and recommended countermeasures, should assist jurisdictions decide which voting systems to certify or purchase, and how to protect those systems from security threats after they have been purchased.

LIMITATIONS OF STUDY

As the first of its kind, this report is necessarily limited in scope. First, it is limited to voting systems that are being widely purchased *today*. The study does not include threat analyses of, most notably, ballot-marking devices,[1] vote by phone systems,[2] or ballot on demand, cryptographic, or witness voting systems.[3] Nor does this study consider early voting or voting that takes place through the mail.[4] We believe that the information and analysis included in this report can be used to perform threat analyses that include these systems and voting methods.

Second, our threat analysis is made in the context of a hypothetical statewide race. There is no reason why the methods used in this analysis cannot be applied to local (or national) races. We believe that such analyses would also be helpful in assisting jurisdictions with certification, purchase, and security decisions, but they were outside the scope of this study.

Third, our study is limited to an analysis of *technology-specific* threats. There are many types of potential attacks on election accuracy and credibility. We have not analyzed technology-neutral threats such as voter intimidation, illegal manipulation of voter rolls, or purges of voter rolls. We believe that such threats must be addressed. Because these threats are not specific to any particular voting system (*i.e.*, they should have the same impact on elections, regardless of the type of system a jurisdiction uses), however, they were not part of our study.

FIGURE 1

VOTING SYSTEMS

Type of Voting System	Description of Voting System (described in f urther detail in Appendix B)	Examples of Voting System
Direct Recording Electronic (DRE)	A DRE machine directly records the voter's selections in each contest, using a ballot that appears on a display screen. Typical DRE machines have flat panel display screens with touch-screen input, although other display technologies have been used. The defining characteristic of these machines is that votes are captured and stored electronically.	Microvote Infinity Voting Panel Hart InterCivic eSlate Sequoia AVC Edge Sequoia AVC Advantage ES&S iVotronic ES&S iVotronic LS Diebold AccuVote-TS Diebold AccuVote-TSX UniLect Patriot
DRE with Voter-Verified Paper Trail (DRE w/VVPT)	A DRE w/VVPT captures a voter's choice both internally in electronic form, and contemporaneously on paper. A DRE w/VVPT allows the voter to confirm the accuracy of the paper record to provide voter-verification.	ES&S iVotronic system with Real Time Audit Log Diebold AccuVote-TSX with AccuView printer Sequoia AVC Edge with VeriVote printer Hart InterCivic eSlate with VVPAT UniLect Patriot with VVPAT
Precinct Count Optical Scan (PCOS)	PCOS voting machines allow voters to mark paper ballots, typically with pencils or pens, independent of any machine. Voters then carry their sleeved ballots to a scanner. At the scanner, they un-sleeve the ballot and insert into the scanner, which optically records the vote.	Diebold AccuVote-OS ES&S Model 100 Sequoia Optech Insight

Fourth, our analysis assumed that certain fundamental physical security and accounting procedures were already in place. Without good procedures, no voting system can be secured. We assumed the operation of a consistent set of procedures drawn from interviews with election officials in order to evaluate the number of informed participants involved in a given attack. All three systems are more vulnerable to attack if appropriate internal controls and procedures are not followed.

All three systems are more vulnerable to attack if appropriate internal controls and procedures are not followed.

Fifth, the report does not address other important factors that must be considered when making decisions about voting systems. Separate from (but concurrent with) its work with the Task Force on Voting System Security, the Brennan Center has completed a series of reports with task forces on voting system accessibility, usability, and cost.[5] In making decisions about their voting systems, jurisdictions must balance their security concerns with important concerns in these other areas.

Finally, our study looks at the ability of persons to successfully execute an attack without detection. Ultimately, it will be up to local jurisdictions to develop clear policies and procedures to ensure that when they find evidence of fraud or accident sufficient to change the outcome of a particular election, appropriate remedial action is taken.

SUMMARY OF FINDINGS AND RECOMMENDATIONS

Three fundamental points emerge from our threat analysis:

- All three voting systems have significant security and reliability vulnerabilities, which pose a real danger to the integrity of national, state, and local elections.
- The most troubling vulnerabilities of each system can be substantially remedied if proper countermeasures are implemented at the state and local level.
- Few jurisdictions have implemented any of the key countermeasures that could make the least difficult attacks against voting systems much more difficult to execute successfully.

Voting System Vulnerabilties

After a review of more than 120 potential threats to voting systems, the Task Force reached the following crucial conclusions:

For *all three* types of voting systems:

- When the goal is to change the outcome of a close statewide election, attacks that involve the insertion of Software Attack Programs or other corrupt software are the least difficult attacks.

- Voting machines that have wireless components are significantly more vulnerable to a wide array of attacks. Currently, only two states, New York and Minnesota, ban wireless components on all voting machines.

For *DREs without* voter-verified paper trails:

- DREs without voter-verified paper trails do not have available to them a powerful countermeasure to software attacks: post-election Automatic Routine Audits that compare paper records to electronic records.

For DREs w/VVPT and PCOS:

- The voter-verified paper record, *by itself*, is of questionable security value. The paper record has significant value only if an Automatic Routine Audit is performed (and a well-designed chain of custody and physical security procedures is followed). Of the 26 states that mandate voter-verified paper records, only 12 require regular audits.

- Even if jurisdictions routinely conduct audits of voter-verified paper records, DREs w/VVPT and PCOS are vulnerable to certain software attacks or errors. Jurisdictions that conduct audits of paper records should be aware of these potential problems.

Security Recommendations

There are a number of steps that jurisdictions can take to address the vulnerabilities identified in the threat analysis and thus to make their voting systems significantly more secure. Specifically, we recommend adoption of the following security measures: [6]

1. Conduct Automatic Routine Audits comparing voter-verified paper records to the electronic record following every election. A voter-verified paper record accompanied by a solid Automatic Routine Audit of those records can go a long way toward making the least difficult attacks much more difficult.

2. Perform "Parallel Testing" (selecting voting machines at random and testing them as realistically as possible) on Election Day. For paperless DREs, in particular, Parallel Testing will help jurisdictions detect software-based attacks as well as subtle software bugs that may not be discovered during inspection and other testing. The Task Force does not recommend Parallel Testing as a substitute for the use of voter-verified paper records with an Automatic Routine Audit.

3. Ban use of voting machines with wireless components. All three voting systems are more vulnerable to attack if they have wireless components.

4. Use a transparent and random selection process for all auditing procedures. For any auditing to be effective (and to ensure that the public is confident in such procedures), jurisdictions must develop and implement transparent and random selection procedures.

5. Ensure decentralized Programming and Voting System administration. Where a single entity, such as a vendor or state or national consultant, performs key tasks for multiple jurisdictions, attacks against statewide elections become easier.

6. Institute clear and effective procedures for addressing evidence of fraud or error. Both Automatic Routine Audits and Parallel Testing are of questionable security value without effective procedures for action where evidence of machine malfunction or fraud is discovered. Detection of fraud without an appropriate response will not prevent attacks from succeeding.

Fortunately, these steps are not particularly complicated or cumbersome. For the most part, they do not involve significant changes in system architecture. Unfortunately, *few jurisdictions have implemented any of the recommended countermeasures.*

Regular examinations of voting system security are necessary because we have *not* always successfully avoided attacks on voting systems

THE NEED FOR A METHODICAL THREAT ANALYSIS

Is an independent study of voting system security really necessary? Have we not managed, in our nation's 230-year history, to avoid the kind of attacks about which certain advocates are suddenly warning?

RECURRENT, SYSTEMATIC THREAT ANALYSES OF VOTING SYSTEMS ARE LONG OVERDUE

The simple answer is that regular examinations of voting system security are necessary because we have *not* always successfully avoided attacks on voting systems – in fact, various types of attacks on voting systems and elections have a "long tradition" in American history.[7] The suspicion or discovery of such attacks has generally provoked momentary outrage, followed by periods of historical amnesia.[8]

In his 1934 book on this issue, Joseph Harris documented numerous cases of attacks on voting systems, including ballot box stuffing, alteration of ballots, substitution of ballots, false counts, posting of false returns, and alteration of returns.[9] More recent examples of tampering with voting systems have been exposed in the last two decades.[10]

In the past, when security and reliability issues surrounding elections have bubbled to the surface of public consciousness, Americans have embraced new technology.[11] It is therefore not particularly surprising that, following the controversial 2000 presidential elections, we have again turned to new voting machines to address our concerns.

These new machines promise great advancements in the areas of accessibility and usability. But all technology, no matter how advanced, is going to be vulnerable to attack to some degree. Many of the vulnerabilities present in our new voting technologies are the same that have always existed; some are new.

The main lesson of the history of attacks on voting systems is that we would be foolish to assume there would not be attacks on voting systems in the future. The best that we can do is understand what vulnerabilities exist and take the proper precautions to ensure that the easiest attacks, with the potential to affect the most votes, are made as difficult as possible.

SOLID THREAT ANALYSES SHOULD HELP MAKE VOTING SYSTEMS MORE RELIABLE

There is an additional benefit to this kind of analysis: it should help make our voting systems more reliable, *regardless of whether they are ever attacked.* Computerized voting systems – like all previous voting systems – have shown themselves vulner-

able to error. Votes have been miscounted or lost as a result of defective firmware,[12] faulty machine software,[13] defective tally server software,[14] election programming errors,[15] machine breakdowns,[16] malfunctioning input devices,[17] and poll worker error.[18]

As Professor Douglas Jones has noted: "An old maxim in the area of computer security is clearly applicable here: Almost everything that a malicious attacker could attempt could also happen by accident; for every malicious attacker, there may be thousands of people making ordinary careless errors."[19] Solid threat analyses should help to expose and to address vulnerabilities in voting systems, not just to security breaches, but also to simple malfunctions that could be avoided.

The main lesson of the history of attacks on voting systems is that we would be foolish to assume there would not be attacks on voting systems in the future.

Firmware is software that is embedded in the voting machine.

Only by prioritizing these various threats could we help election officials identify which attacks they should be most concerned about, and what steps could be taken to make such attacks as difficult as possible.

METHODOLOGY

The Task Force concluded, and the peer review team at NIST agreed, that the best approach for comprehensively evaluating voting system threats was to: (1) identify and categorize the potential threats against voting systems, (2) prioritize these threats based upon an agreed upon metric (which would tell us how difficult each threat is to accomplish from the attacker's point of view), and (3) determine, utilizing the same metric employed to prioritize threats, how much more difficult each of the catalogued attacks would become after various sets of countermeasures are implemented.

This model allows us to identify the attacks we should be most concerned about (*i.e.*, the most practical and least difficult attacks). Furthermore, it allows us to quantify the potential effectiveness of various sets of countermeasures (*i.e.*, how difficult the least difficult attack is after the countermeasure has been implemented). Other potential models considered, but ultimately rejected by the Task Force, are detailed in Appendix A.

IDENTIFICATION OF THREATS

The first step in creating a threat model for voting systems was to identify as many potential attacks as possible. To that end, the Task Force, together with the participating election officials, spent several months identifying voting system vulnerabilities. Following this work, NIST held a Voting Systems Threat Analysis Workshop on October 7, 2005. Members of the public were invited to write up and post additional potential attacks. Taken together, this work produced over 120 potential attacks on the three voting systems. They are detailed in the catalogs.[20] Many of the attacks are described in more detail at http://vote.nist.gov/threats/papers.htm.

The types of threats detailed in the catalogs can be broken down into nine categories: (1) the insertion of corrupt software into machines prior to Election Day; (2) wireless and other remote control attacks on voting machines on Election Day; (3) attacks on tally servers; (4) miscalibration of voting machines; (5) shut-off of voting machine features intended to assist voters; (6) denial-of-service attacks; (7) actions by corrupt poll workers or others at the polling place to affect votes cast; (8) vote-buying schemes; and (9) attacks on ballots or VVPT. Often, the actual attacks involve some combination of these categories. We provide a discussion of each type of attack in "Nine Categories of Attacks," *infra* pp. 24–27.

PRIORITIZING THREATS: NUMBER OF INFORMED PARTICIPANTS AS METRIC

Without some form of prioritization, a compilation of the threats is of limited value. Only by prioritizing these various threats could we help election officials identify which attacks they should be most concerned about, and what steps

could be taken to make such attacks as difficult as possible. As discussed below, we have determined the level of difficulty for each attack where the attacker is attempting to affect the outcome of a close statewide election.[21]

There is no perfect way to determine which attacks are the least difficult, because each attack requires a different mix of resources – well-placed insiders, money, programming skills, security expertise, *etc.* Different attackers would find certain resources easier to acquire than others. For example, election fraud committed by local election officials would always involve well-placed insiders and a thorough understanding of election procedures; at the same time, there is no reason to expect such officials to have highly skilled hackers or first-rate programmers working with them. By contrast, election fraud carried out by a foreign government would likely start with plenty of money and technically skilled attackers, but probably without many conveniently placed insiders or detailed knowledge of election procedures.

Ultimately, we decided to use the "number of informed participants" as the metric for determining attack difficulty. An attack which uses fewer participants is deemed the easier attack.

We have defined "informed participant" as someone whose participation is needed to make the attack work, and who knows enough about the attack to foil or expose it. This is to be distinguished from a participant who unknowingly assists the attack by performing a task that is integral to the attack's successful execution without understanding that the task is part of an attack on voting systems.

The reason for using the security metric "number of informed participants" is relatively straightforward: the larger a conspiracy is, the more difficult it would be to keep it secret. Where an attacker can carry out an attack by herself, she need only trust herself. On the other hand, a conspiracy that requires thousands of people to take part (like a vote-buying scheme) also requires thousands of people to keep quiet. The larger the number of people involved, the greater the likelihood that one of them (or one who was approached, but declined to take part) would either inform the public or authorities about the attack, or commit some kind of error that causes the attack to fail or become known.

Moreover, recruiting a large number of people who are willing to undermine the integrity of a statewide election is also presumably difficult. It is not hard to imagine two or three people agreeing to work to change the outcome of an election. It seems far less likely that an attacker could identify and employ hundreds or thousands of similarly corrupt people without being discovered.

We can get an idea of how this metric works by looking at one of the threats listed in our catalogs: the vote-buying threat, where an attacker or attackers pay individuals to vote for a particular candidate. This is Attack Number 26 in the PCOS Attack Catalog[22] (though this attack would not be substantially different against

While practical in smaller contests, a vote-buying attack would be an exceptionally difficult way to affect the outcome of a statewide election.

DREs or DREs w/VVPT).[23] In order to work under our current types of voting systems, this attack requires (1) at least one person to purchase votes, (2) many people to agree to sell their votes, and (3) some way for the purchaser to confirm that the voters she pays actually voted for the candidate she supported. Ultimately, we determined that, while practical in smaller contests, a vote-buying attack would be an exceptionally difficult way to affect the outcome of a statewide election. This is because, even in a typically close statewide election, an attacker would need to involve thousands of voters to ensure that she could affect the outcome of a statewide race.[24]

For a discussion of other metrics we considered, but ultimately rejected, *see* Appendix C.

DETERMINING NUMBER OF INFORMED PARTICIPANTS

DETERMINING THE STEPS AND VALUES FOR EACH ATTACK

The Task Force members broke down each of the catalogued attacks into its necessary steps. For instance, Attack Number 12 in the PCOS Attack Catalog is "Stuffing Ballot Box with Additional Marked Ballots."[25] We determined that, at a minimum, there were three component parts to this attack: (1) stealing or creating the ballots and then marking them, (2) scanning marked ballots through the PCOS scanners, probably before the polls opened, and (3) modifying the poll books in each location to ensure that the total number of votes in the ballot boxes was not greater than the number of voters who signed in at the polling place.

Task Force members then assigned a value representing the minimum number of persons they believed would be necessary to accomplish each goal. For PCOS Attack Number 12, the following values were assigned:[26]

Minimum number required to steal or create ballots: 5 persons total.[27]

Minimum number required to scan marked ballots: 1 person per polling place attacked.

Minimum number required to modify poll books: 1 person per polling place attacked.[28]

After these values were assigned, the Brennan Center interviewed several election officials to see whether they agreed with the steps and values assigned to each attack.[29] When necessary, the values and steps were modified. The new catalogs, including attack steps and values, were then reviewed by Task Force members. The purpose of this review was to ensure, among other things, that the steps and values were sound.

These steps and values tell us how difficult it would be to accomplish a *single attack in a single polling place.* They do not tell us how many people it would take to change

the outcome of an election successfully – that depends, of course, on specific facts about the jurisdiction: how many votes are generally recorded in each polling place, how many polling places are there in the jurisdiction, and how close is the race? For this reason, we determined that it was necessary to construct a hypothetical jurisdiction, to which we now turn.

NUMBER OF INFORMED PARTICIPANTS NEEDED TO CHANGE STATEWIDE ELECTION

We have decided to examine the difficulty of each attack in the context of changing the outcome of a reasonably close statewide election. While we are concerned by potential attacks on voting systems in any type of election, we are most troubled by attacks that have the potential to affect large numbers of votes. These are the attacks that could actually change the outcome of a statewide election with just a handful of attack participants.

We are less troubled by attacks on voting systems that can only affect a small number of votes (and might therefore be more useful in local elections). This is because there are many non-system attacks that can also affect a small number of votes (*i.e.,* sending out misleading information about polling places, physically intimidating voters, submitting multiple absentee ballots, *etc.*). Given the fact that these non-system attacks are likely to be less difficult in terms of number of participants, financial cost, risk of detection, and time commitment, we are uncertain that an attacker would target *voting machines* to alter a small number of votes.

In order to evaluate how difficult it would be for an attacker to change the outcome of a statewide election, we created a composite jurisdiction. The composite jurisdiction was created to be representative of a relatively close statewide election. We did not want to examine a statewide election where results were so skewed toward one candidate (for instance, the re-election of Senator Edward M. Kennedy in 2000, where he won 73% of the vote[30]), that reversing the election results would be impossible without causing extreme public suspicion. Nor did we want to look at races where changing only a relative handful of votes (for instance, the governor's race in Washington State in 2004, which was decided by a mere 129 votes[31]) could affect the outcome of an election; under this scenario, many of the potential attacks would involve few people, and therefore look equally difficult.

We have named our composite jurisdiction "the State of Pennasota." The State of Pennasota is a composite of ten states: Colorado, Florida, Iowa, Ohio, New Mexico, Pennsylvania, Michigan, Nevada, Wisconsin and Minnesota. These states were chosen because they were the ten "battleground" states that Zogby International consistently polled in the spring, summer, and fall 2004.[32] These are statewide elections that an attacker would have expected, ahead of time, to be fairly close.

We have also created a composite election, which we label the "Governor's Race" in Pennasota. The results of this election are a composite of the actual results in the same ten states in the 2004 Presidential Election.

We have used these composites as the framework by which to evaluate the difficulty of the various catalogued attacks.[33] For instance, we know a ballot-box stuffing attack would require roughly five people to create and mark fake ballots, as well as one person per polling place to stuff the boxes, and one person per polling place to modify the poll books. But, in order to determine how many informed participants would be needed to affect a statewide race, we need to know how many polling places would need to be attacked.

The composite jurisdiction and composite election provide us with information needed to answer these questions: *i.e.*, how many extra votes our attackers would need to add to their favored candidate's total for him to win, how many ballots our attackers can stuff into a particular polling place's ballot box without arousing suspicion (and related to this, how many votes are generally cast in the average polling place), how many polling places are there in the state, *etc.* We provide details about both the composite jurisdiction and election in the section entitled "Governor's Race, State of Pennasota, 2007," *infra* pp. 20–23.

LIMITS OF INFORMED PARTICIPANTS AS METRIC

Of the possible metrics we considered, we believe that measuring the number of people who know they are involved in an attack (and thus could provide evidence of the attack to the authorities and/or the media), is the best single measure of attack difficulty; as already discussed, we have concluded that the more people an attacker is forced to involve in his attack, the more likely it is that one of the participants would reveal the attack's existence and foil the attack, perhaps sending attackers to jail. However, we are aware of a number of places where the methodology could provide us with questionable results.

Steganography is "the art and science of writing hidden messages in such a way that no one apart from the intended recipient knows of the existence of the message."

By deciding to concentrate on the size of an attack team, we mostly ignore the need for other resources when planning an attack. Thus, a software attack on DREs which makes use of steganography[34] to hide attack instruction files (*see* "DRE w/VVPT Attack Number 1a," discussed in greater detail, *infra* pp. 62–64) is considered easier than an attack program delivered over a wireless network at the polling place (*see* discussion of wireless networks, *infra* pp. 85–86). However, the former attack probably requires a much more technologically sophisticated attacker.

Another imperfection with this metric is that we do not have an easy way to represent how much choice the attacker has in finding members of his attack team. Thus, with PCOS voting, we conclude that the cost of subverting a routine audit of ballots is roughly equal to the cost of intercepting ballot boxes in transit and substituting altered ballots (*see* discussion of PCOS attacks, *infra* pp. 77–84).

However, subverting the audit team requires getting a specific set of trusted people to cooperate with the attacker. By contrast, the attacker may be able to decide which precincts to tamper with based on which people she has already recruited for her attack.

In an attempt to address this concern, we considered looking at the number of "insiders" necessary to take part in each attack. Under this theory, getting five people to take part in a conspiracy to attack a voting system might not be particularly difficult. But getting five well-placed county election officials to take part in the attack would be (and should be labeled) the more difficult of the two attacks. Because, for the most part, the low-cost attacks we have identified do not necessarily involve well placed insiders (but could, for instance, involve one of many people with access to commercial off-the-shelf software ("COTS") during development or at the vendor), we do not believe that using this metric would have substantially changed our analysis.[35]

Finally, these attack team sizes do not always capture the logistical complexity of an attack. For example, an attack on VVPT machines involving tampering with the voting machine software and also replacing the paper records in transit requires the attacker to determine what votes were falsely produced by the voting machine and print replacement records in time to substitute them. While this is clearly possible, it raises a lot of operational difficulties – a single failed substitution leaves the possibility that the attack would be detected during the audit of ballots.

We have tried to keep these imperfections in mind when analyzing and discussing our least difficult attacks.

We suspect that much of the disagreement between voting officials and computer security experts in the last several years stems from a difference of opinion in prioritizing the difficulty of attacks. Election officials, with extensive experience in the logistics of handling tons of paper ballots, have little faith in paper and understand the kind of breakdowns in procedures that lead to traditional attacks like ballot box stuffing; in contrast, sophisticated attacks on computer voting systems appear very difficult to many of them. Computer security experts understand sophisticated attacks on computer systems and recognize the availability of tools and expertise that makes these attacks practical to launch, but have no clear idea how they would manage the logistics of attacking a paper-based system. Looking at attack team size is one way to bridge this difference in perspective.

EFFECTS OF IMPLEMENTING COUNTERMEASURE SETS

The final step of our threat analysis is to measure the effect of certain countermeasures against the catalogued attacks. How much more difficult would the attacks become once the countermeasures are put into effect? How many more informed participants (if any) would be needed to counter or defeat these countermeasures?

Our process for examining the effectiveness of a countermeasure mirrors the process for determining the difficulty of an attack: we first asked whether the countermeasure would allow us to detect an attack with near certainty. If we agreed that the countermeasure would expose the attack, we identified the steps that would be necessary to circumvent or defeat the countermeasure. For each step to defeat the countermeasure, we determined the number of additional informed participants (if any) that an attacker would need to add to his team.

As with the process for determining attack difficulty, the Brennan Center interviewed numerous election officials to see whether they agreed with the steps and values assigned. When necessary, the values and steps for defeating the countermeasures were altered to reflect the input of election officials.

COUNTERMEASURES EXAMINED

BASIC SET OF COUNTERMEASURES

The first set of countermeasures we looked at is the "Basic Set" of countermeasures. This Basic Set was derived from security survey responses[36] we received from county election officials around the country, as well as additional interviews with more than a dozen current and former election officials. Within the Basic Set of countermeasures are the following procedures:

Inspection

- The jurisdiction is not knowingly using any uncertified software that is subject to inspection by the Independent Testing Authority (often referred to as the "ITA").[37]

Physical Security for Machines

- Ballot boxes (to the extent they exist) are examined (to ensure they are empty) and locked by poll workers immediately before the polls are opened.
- Before and after being brought to the polls for Election Day, voting systems for each county are locked in a single room, in a county warehouse.
- The warehouse has perimeter alarms, secure locks, video surveillance and regular visits by security guards.
- Access to the warehouse is controlled by sign-in, possibly with card keys or similar automatic logging of entry and exit for regular staff.
- Some form of "tamper-evident" seals are placed on machines before and after each election.

- The machines are transported to polling locations five to fifteen days before Election Day.

Chain of Custody/Physical Security of Election Day Records

- At close of the polls, vote tallies for each machine are totaled and compared with number of persons that have signed the poll books.
- A copy of totals for each machine is posted at each polling place on election night and taken home by poll workers to check against what is posted publicly at election headquarters, on the web, in the papers, or elsewhere.[38]
- All audit information (*i.e.*, Event Logs, VVPT records, paper ballots, machine printouts of totals) that is not electronically transmitted as part of the unofficial upload to the central election office, is delivered in official, sealed and hand-delivered information packets or boxes. All seals are numbered and tamper-evident.
- Transportation of information packets is completed by two election officials representing opposing parties who have been instructed to remain in joint custody of the information packets or boxes from the moment it leaves the precinct to the moment it arrives at the county election center.
- Each polling place sends its information packets or boxes to the county election center separately, rather than having one truck or person pick up this data from multiple polling locations.
- Once the sealed information packets or boxes have reached the county election center, they are logged. Numbers on the seals are checked to ensure that they have not been replaced. Any broken or replaced seals are logged. Intact seals are left intact.
- After the packets and/or boxes have been logged, they are provided with physical security precautions at least as great as those listed for voting machines, above. Specifically, for Pennasota, we have assumed that the room in which the packets are stored has perimeter alarms, secure locks, video surveillance and regular visits by security guards and county police officers, and that access to the room is controlled by sign-in, possibly with card keys or similar automatic logging of entry and exit for regular staff.

Testing[39]

- An Independent Testing Authority has certified the model of voting machine used in the polling place.

- Acceptance Testing[40] is performed on machines at the time, or soon after, they are received by the County.

- Pre-election Logic and Accuracy[41] testing is performed by the relevant election official.

- Prior to opening the polls, every voting machine and vote tabulation system is checked to see that it is still configured for the correct election, including the correct precinct, ballot style, and other applicable details.

REGIMEN FOR AUTOMATIC ROUTINE AUDIT PLUS BASIC SET OF COUNTERMEASURES.

The second set of countermeasures is the Regimen for an Automatic Routine Audit Plus Basic Set of Countermeasures.

Some form of routine auditing of voter-verified paper records to test the accuracy of electronic voting machines occurs in 12 states. They generally require that between 1 and 10% of all precinct voting machines be audited after each election.[42]

Jurisdictions can implement this set of countermeasures only if their voting systems produce some sort of voter-verified paper record of each vote. This could be in the form of a paper ballot, in the case of PCOS, or a voter-verified paper trail ("VVPT"), in the case of DREs.

We have assumed that jurisdictions take the following steps when conducting an Automatic Routine Audit (when referring to this set of assumptions "Regimen for an Automatic Routine Audit"):

The Audit

- Leaders of the major parties in each county are responsible for selecting a sufficient number of audit-team members to be used in that county.[43]

- Using a highly transparent random selection mechanism (*see infra* p. 17), the voter-verified paper records for a small percentage of all voting machines in the State are selected for auditing.

- Using a transparent random selection method, auditors are assigned to the selected machines (two or three people, with representatives of each major political party, would comprise each audit team).

- The selection of voting machines and the assignment of auditors to machines occurs immediately before the audit takes place. The audit takes place as

soon as possible after polls close – for example, at 9 a.m. the morning after polls close.

- Using a transparent random selection method, county police officers, security personnel and the video monitor assigned to guard the voter-verified records are chosen from a large pool of on-duty officers and employees on election night.

- The auditors are provided the machine tallies and are able to see that the county tally reflects the sums of the machine tallies before the start of the inspection of the paper.

- The audit would include a tally of spoiled ballots (in the case of VVPT, the number of cancellations recorded), overvotes, and undervotes.

Transparent Random Selection Process

In this report, we have assumed that random auditing procedures are in place for both the Regimen for an Automatic Routine Audit and Regimen for Parallel Testing (*See infra* p. 18). We have further assumed procedures to prevent a single, corrupt person from being able to fix the results. This implies a kind of transparent and public random procedure.

For the Regimen for an Automatic Routine Audit there are at least two places where transparent, random selection processes are important: in the selection of precincts to audit and in the assignment of auditors to the precincts they will be auditing.

Good election security can employ Transparent Random Selection in other places with good effect:

- The selection of parallel testers from a pool of qualified individuals.

- The assignment of police and other security professionals from on-duty lists to monitor key materials, for example, the VVPT records between the time that they arrive at election central and the time of the completion of the Automatic Routine Audit.

If a selection process for auditing is to be trustworthy and trusted, ideally:

- The whole process will be publicly observable or videotaped;[44]

- The random selection will be publicly verifiable, *i.e.*, anyone observing will be able to verify that the sample was chosen randomly (or at least that the number selected is not under the control of any small number of people); and

- The process will be simple and practical within the context of current election practice so as to avoid imposing unnecessary burdens on election officials.

There are a number of ways that election officials can ensure some kind of transparent randomness. One way would be to use a state lottery machine to select precincts or polling places for auditing. We have included two potential examples of transparent random selection processes in Appendix F. These apply to the Regimen for Parallel Testing as well.

REGIMEN FOR PARALLEL TESTING PLUS BASIC SET OF COUNTERMEASURES

The final set of countermeasures we have examined is the Regimen for Parallel Testing Plus Basic Set of Countermeasures. Parallel Testing, also known as election-day testing, involves selecting voting machines at random and testing them as realistically as possible during the period that votes are being cast.

Parallel Testing

In developing our set of assumptions for Parallel Testing, we relied heavily upon interviews with Jocelyn Whitney, Project Manager for Parallel Testing in the State of California, and conclusions drawn from this Report.[45] In our analysis, we assume that the following procedures would be included in the Parallel Testing regimen (when referring to this regimen "Regimen for Parallel Testing") that we evaluate:

- At least two of each DRE model (meaning both vendor and model) would be selected for Parallel Testing.
- At least two DREs from each of the three largest counties would be parallel tested.
- Counties to be parallel tested would be chosen by the Secretary of State in a transparent and random manner.
- Counties would be notified as late as possible that machines from one of their precincts would be selected for Parallel Testing.[46]
- Precincts would be selected through a transparent random mechanism.
- A video camera would record testing.
- For each test, there would be one tester and one observer.
- Parallel Testing would occur at the polling place.

- The script for Parallel Testing would be generated in a way that mimics voter behavior and voting patterns for the polling place.

- At the end of the Parallel Testing, the tester and observer would reconcile vote totals in the script with vote totals reported on the machine.

Transparent Random Selection Process

We further assume that the same type of transparent random selection process that would be used for the Regimen for Automatic Routine Audit would also be employed for the Regimen for Parallel Testing to determine which machines would be subjected to testing on Election Day.

REPRESENTATIVE MODEL FOR EVALUATING ATTACKS AND COUNTERMEASURES: GOVERNOR'S RACE, STATE OF PENNASOTA, 2007

In this section, we provide the assumptions that we have made concerning (1) the governor's race in the State of Pennasota, and (2) the limitations that our attacker would face in attempting to subvert that election.

FACTS ABOUT PENNASOTA

In creating our assumptions for the Pennasota's gubernatorial race, we have averaged the results of the 2004 Presidential Election in ten "battleground" states. Based upon this average, we have assumed that 3,459,379 votes would be cast in Pennasota's gubernatorial election. The average margin of victory in the 10 battleground states was 2.3%. Accordingly, we assumed that this would be the margin of victory between the two main candidates in our hypothetical election (in total votes, this is 80,257).

FIGURE 2

ELECTION FOR GOVERNOR, STATE OF PENNASOTA, 2007

Candidate	Party	Total Votes	Percentage of Votes
Tom Jefferson	Dem-Rep	1,769,818	51.1
Johnny Adams	Federalists	1,689,650	48.8

A table that documents all of the relevant numbers for Pennasota and the 2007 gubernatorial election is provided in Appendix G.[49]

EVALUATING ATTACKS IN PENNASOTA

To complete our analysis, we ran each attack through the 2007 governor's race in Pennasota. The goal was to determine how many informed participants would be needed to move the election from Tom Jefferson to Johnny Adams.

We have assumed that our attacker would seek to change these results so that Johnny Adams is assured victory. Accordingly, although the election is decided by 2.3% of the vote, we have calculated that the attacker's goal is to (1) add 3.0% (or 103,781 votes) to Johnny Adams total, (2) subtract 3.0% of the total votes from Tom Jefferson, or (3) switch 1.5% (or 51,891 votes) from Tom Jefferson to Johnny Adams. [50]

By examining a particular attack in the context of our goal of changing the results of Pennasota's 2007 governor's race, it becomes clear how difficult an attack actually would be. Earlier, we assigned the following steps and values for

PCOS Attack 12 ("Stuffing Ballot Box with Additional Marked Ballots"):

Minimum number required to steal or create ballots:[51] 5 persons total

Minimum number required to scan the ballots: 1 person per polling place attacked.

Minimum number required to modify poll books: 1 person per polling place attacked.

Our attacker seeks to use the "ballot-stuffing attack" to add 103,781 votes to Johnny Adams' total. There are approximately 1142 voters per polling place in the State of Pennasota.[52] Theoretically, our attacker could add 103,781 votes for Johnny Adams in the boxes of three or four polling places and her favored candidate would win. In this case, she would only need to involve a dozen people (including herself) to carry out the attack successfully: five to create the ballots, three or four to stuff the boxes, and three or four to modify (and add to) the poll books.

As a practical matter, of course, this attempt at ballot stuffing would not work. Someone (and, more likely, many people) would notice if a few polling places that normally recorded 1100–1200 votes were suddenly reporting 25,000 votes each for Johnny Adams.

We have assumed that in order to avoid detection our attacker could add no more than 15% of the total votes in a particular polling place for Johnny Adams (*see* "Limits on Attacker," *infra* p. 22, for further discussion). Accordingly, our formula for determining how many polling places she must target is as follows:

number of
polling places targeted = (total votes that must be added) /
[(total number of votes per polling place) ×
(percent that may be taken from any polling place)]

or, in actual numbers:

number of
polling places targeted = 103,781 / (1,142 × 15%) = 606

From this we learn that attempting to change a statewide election by scanning in extra marked ballots would be extremely difficult. More specifically, it would likely require more than 1,000 informed participants: 5 to create/steal and mark the appropriate ballots, plus 606 to place ballots in separate ballot boxes in each polling place, plus 606 to modify the poll books in each polling place. It is unlikely that (1) an attacker could find so many people willing to participate in such an attack without inadvertently soliciting someone who would expose the plot, (2) all 1,000 participants would keep silent about the attack, and (3) even if all 1,000 solicited persons agreed to take part in the attack, and none of them purposefully exposed the plot, that no one would get caught perpetrating the conspiracy.[53]

LIMITS ON ATTACKER

We have assumed that our attacker would prefer that her actions not raise undue suspicion. Accordingly, we have placed some limits on the type of actions our attacker could take. As just demonstrated by looking at the ballot-stuffing attack, these limits can further help us determine how difficult a particular attack would be (*i.e.,* how many informed participants the attacker would need to involve).

Perhaps most importantly, we have assumed our attacker would not want to add or subtract more than 10% of the votes for a candidate in any one county (or switch more than 5% from one candidate to another), for fear that a greater change would attract suspicion. We believe that this is a conservative estimate, but the reason for creating some kind of cap should be obvious: if enough votes are switched in a specific location, it would eventually become apparent that something has gone wrong (whether through fraud or error).

We can see this by looking at a specific example from an actual election. In 2004, in heavily Democratic Cook County, Illinois, John Kerry received 59% of the vote and George Bush received 40%.[54] It is unlikely that, just by looking at vote totals for Cook County, anyone would have assumed that there was fraud or error if John Kerry received 63% or 55% of the countywide vote. On the other hand, if John Kerry received less than 50% or more than 70% of the vote in Cook County, these totals would (at the very least) attract attention and increase the likelihood that there would be some investigation. This would be particularly true if John Kerry's totals were otherwise within reasonable expectations in other counties in Illinois and around the country. An attacker would seek to avoid such an extraordinary aberration.

For the same reasons, we have put limits on the number of votes an attacker would seek to change in a single polling place or a single machine. We have assumed that a swing of greater than 15% in any single polling place or 30% on any single machine would attract too much suspicion. Therefore, an attacker would avoid adding or subtracting more than these numbers of votes per polling place and machine.[55]

FIGURE 3

ASSUMED PRECAUTIONS TAKEN BY ATTACKER:
LIMITS ON THE % OF VOTES ADDED OR SUBTRACTED FOR A CANDIDATE

Maximum % Votes Added or Subtracted Per County	10% (5% switch)
Maximum % Votes Added or Subtracted Per Polling Place	15% (7.5% switch)
Maximum % Votes Added or Subtracted Per Voting Machine	30% (15% switch)

TARGETING THE FEWEST COUNTIES

As will be discussed, *infra* pp. 71–74, many attacks would be easier to execute, and more difficult to detect, if they were limited to a small number of counties or polling places. Given the limits we have set on our attacker, we have concluded that, to change enough votes to affect the outcome of our statewide election, she would have to attack a minimum of three counties.[56] These would be the three largest counties in the State of Pennasota (where there are enough votes to swing the statewide election).[57] This conclusion is supported in the table below.

We ran our threat analysis against the results of the 2004 presidential race in Florida, New Mexico and Pennsylvania.

FIGURE 4
TOTAL VOTES JOHNNY ADAMS NEEDS TO SWITCH TO ENSURE VICTORY: 51,891

	Actual Vote[58]	Number of Votes Switched	% of County Votes Switched	New Total
Mega County		23,453	4.4%	
Jefferson (D-R)	194,848			171,395
Adams (F)	336,735			360,188
Capitol County		17,306	4.8%	
Jefferson (D-R)	157,985			140,679
Adams (F)	202,556			219,862
Suburbia County		11,132	4.2%	
Jefferson (D-R)	128,933			117,801
Adams (F)	135,003			146,135
Statewide Totals		51,891		
Jefferson (D-R)	1,769,818			1,717,927
Adams (F)	1,689,561			1,741,452

TESTING THE ROBUSTNESS OF OUR FINDINGS

To ensure that the results of our analysis were robust and not limited to the composite jurisdiction of Pennasota, we ran our threat analysis against the results of the 2004 presidential race in Florida, New Mexico and Pennsylvania, and came up with substantially similar conclusions. Specifically, all of the findings and recommendations in the Introduction (*supra* pp. 1–5) still applied.

We also re-ran our analysis in Pennasota, but changed the limits on our attacker, allowing her to change many more votes on a single machine and attempt to change the governor's race in a single (*i.e.*, "Mega") county. Again, all eight of the findings listed in the Introduction still applied.

24

THE CATALOGS

As already discussed, we have catalogued over 120 potential attacks on voting systems. These fall into nine categories, which cover the diversity and breadth of voting machine vulnerabilities.[39]

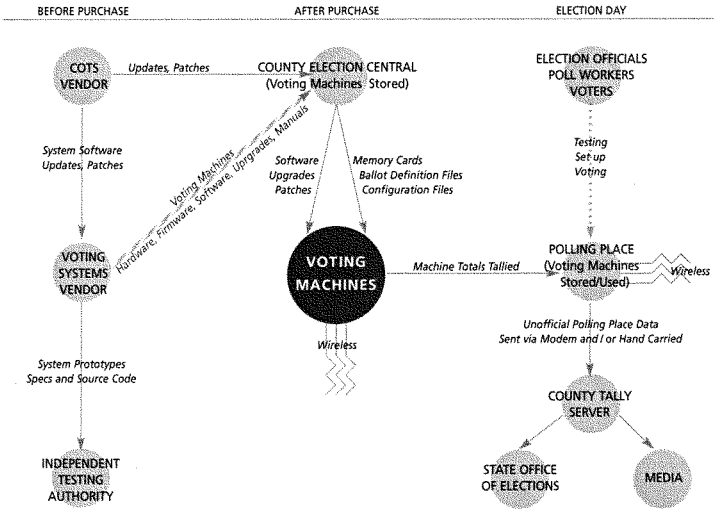
NINE CATEGORIES OF ATTACKS

One way of thinking about the voting process is to view it as a flow of information: the vendor and programmers present the voter with information about her election choices via the voting machine; the voter provides the voting machine with her choices; the voter's choice is then tallied by the voting machines, and this tallied information is (at the close of the polls) provided to poll workers; from the polling place, the vote tallies (whether in paper, electronic, or both forms) from all voting machines are sent to a county tally center; from there countywide totals are reported to state election officials and the media.

Attacks on voting systems are attacks on this flow of information. If we view the nine categories in the context of this flow, we get a better idea of how they might be accomplished.

FIGURE 5

TYPICAL FLOW OF INFORMATION TO AND FROM VOTING MACHINES



1. The Insertion of Corrupt Software Into Machines Prior to Election Day. This is an attack on the voting machine itself, and it occurs before the voting machine even reaches the polling place. Someone with access to voting machines, software, software updates, or devices inserted into voting machines (such as printers or memory cards) introduces corrupt software (such as an Attack Program) that forces the machine to malfunction in some way. We can see by looking at the chart that there are several points of attack that exist before a machine reaches the polling place. The malfunction triggered by the corrupt software could, among other things, cause the machine to misrecord votes, add or lose votes, skip races, perform more slowly or break down altogether.

One challenge associated with this attack is that it is likely to be operationally and technically difficult to carry out successfully. A second problem is that, because this attack occurs *before* Election Day, the attacker would not necessarily have the flexibility to adjust her attack to new facts learned immediately before or on Election Day (such as changes in the dynamics of the race, including which candidates are running or how many votes are likely to be needed to ensure a particular outcome). This type of attack is discussed in "Software Attacks on Voting Machines," *infra* pp. 30–47).

2. Wireless and Other Remote Control Attacks. This is also a direct attack on the voting machine. But unlike the "Insertion of Corrupt Software" attack discussed above, this attack can happen on, or immediately before, Election Day (it could also happen much earlier).

This type of attack is often imagined in conjunction with corrupt software attacks. Machines with wireless components are particularly vulnerable to such attacks. Using a wireless PDA or any other device that allows one to access wireless networks, an attacker could instruct a machine to activate (or turn off) a Software Attack Program, send its own malicious instructions, or attempt to read data recorded by the machine.

Personal digital assistants (PDAs or palmtops) are handheld devices orignally designed as personal organizers. PDAs can synchronize data wirelessly with a computer.

3. Attacks on Tally Servers. The tally server is a central tabulator which calculates the total votes for a particular jurisdiction (generally at the county level). This attack would occur after the polls have closed and the machines have recorded votes.

An attack on a tally server could be direct (*e.g.,* on the database that totals votes) or indirect (*e.g.,* by intercepting a communication *to* the server). In either case, the attacker would attempt to change or delete the totals reported by the tally server, or the data used to compute those totals.

4. Miscalibration of Machines. All three voting systems use some method to interpret and electronically record the voter's choice. At the close of an election, the machine reports (in electronic and printed form) its tally of the votes. For all three systems, if a machine is not calibrated correctly, it could favor one candidate over another.

We can use the DRE as an example. Let us return to the governor's race in Pennasota: in that race, a touch on the left half of the DRE screen should be recorded as a vote for Tom Jefferson; a vote on the right half of the screen should be recorded as a vote for Johnny Adams. The DRE could be miscalibrated so that touches on the left side, close to the center of the screen, are recorded for Johnny Adams rather than Tom Jefferson.

An obvious problem with this specific example is that most voters who pressed "Jefferson" close to the center of the screen would note on the confirmation screen that their vote had been misrecorded; they would reject the Adams vote and try again. But some might not notice that their vote was misrecorded. In these cases, the miscalibration would take votes away from Jefferson and add votes to Adams' total.

5. Shut Off Voting Machine Features Intended to Assist Voters. This is another attack that is directed at the machine itself. For all three systems, there are many features that are intended to assist voters in ensuring that their choices are recorded correctly. By disabling one of these features, an attacker can ensure that some votes would not be accurately recorded.

By way of example, let us return to Pennasota, but this time consider the PCOS machine. PCOS machines have an over/undervote protection that is intended to make sure that voters vote in every race. If a voter accidentally votes for two candidates in the governor's race, the scanner should return the ballot to her without recording any votes. Until she erases one of her choices for governor, or indicates to the machine that she does not want her vote for governor to count, her ballot would not be recorded.

If our attacker is a poll worker who wants Adams to win and works in a polling place where nearly all voters *intend* to vote for Jefferson, she could manually shut off the over/undervote protection. Given the fact that most voters in this polling place want to vote for Jefferson, the chances are that Jefferson would lose some votes as a result. As with the miscalibration attack, this attack does not have to be manual; a Software Attack Program inserted before Election Day could also attempt to shut off such machine functions.

6. Denial-of-Service Attacks. This covers a broad range of attacks. In essence, this attack is meant to keep people from voting, by making it difficult or impossible to cast a vote on a machine. The attack could be lodged directly upon the machine: for instance, by insertion of corrupt software, as discussed above, or by physically destroying a machine or machines.

Again, looking at the governor's race in Pennasota, our attacker would likely target machines and polling places where she knows most voters would support Tom Jefferson.

7. Actions by Corrupt Poll Workers or Others at the Polling Place to Affect Votes Cast. In our catalogs, these attacks range from activating a Software Attack Program already inserted into a voting machine, to shutting off voting machine functions (discussed above), to giving poor instructions or misleading information to certain voters. It could involve an attack on the machines themselves, upon voters, or upon information meant to be transported from polling places to tally centers. This attack could also include providing incomplete or inaccurate instruction to poll workers.

8. Vote-Buying Schemes. This type of attack was already discussed, *supra* pp. 9–10. As noted, such attacks would require so many informed participants that they are unlikely to affect a statewide election without being exposed.

9. Attacks on Ballots or VVPT. This type of attack could occur at many points. Some jurisdictions purchase their ballots directly from a vendor. Others get their ballots from the county election office. In either case, ballots could be tampered with before they reach the polling place. Both ballots and the VVPT could be tampered with at the polling place, or as they are transported to the county tally center. Finally, in states that have Automatic Routine Audits or recounts of voter-verified paper records, ballots and VVPT could be tampered with prior to the audit at the county offices or tally center.

LESSONS FROM THE CATALOGS: RETAIL ATTACKS SHOULD NOT CHANGE THE OUTCOME OF MOST CLOSE STATEWIDE RACES

The least difficult attacks are centralized attacks that occur against the entire voting system.

The catalogs show us that it is very difficult[60] to successfully change the outcome of a statewide election by implementing "retail" attacks on a large scale. Retail attacks are attacks that occur at individual polling places, or during the transport of hardware and/or ballots to and from individual polling places. We have found that these attacks would require too many participants and garner too few votes to have a good chance of swinging a statewide election like the governor's race in Pennasota.

In contrast, the least difficult attacks are centralized attacks that occur against the entire voting system. These attacks allow an attacker to target many votes with few fellow conspirators.

To see why retail attacks are unlikely to change the outcome of most close statewide elections, it is useful to look to see how a typical retail threat listed in our catalog might affect the totals in Pennasota's governor's race. Attack 20 in the DRE w/VVPT catalog is the "Paper Trail Boycott" attack.[61] In this attack, an attacker would enlist voters in polling places where her favored candidate is expected to do poorly. Each of the enlisted voters complains to the poll workers that no matter how many times the voter tries, the paper trail record never corresponds to his choices. The election officials would have no choice but to remove

the "offending" machines from service. This would reduce the number of available machines, creating a "bottleneck" where voters would have to wait in long lines. Ultimately, some voters would give up and leave the lines without voting.

There is one step to this attack, but it must be repeated many times: voters must falsely complain that the machines are not recording their votes correctly.

Again, we assume that the conspiring voters would want Tom Jefferson to lose a net total of 103,781 votes (there is no switching of votes in this scenario; the attackers hope is that their bottleneck would prevent many of Tom Jefferson's supporters from voting, thus reducing his vote total).

We have assumed that if five voters in a short period of time report that the same machine is not recording their vote correctly, poll workers would be forced to shut it down. As already discussed, the average number of voters per polling place in the State of Pennasota is 1142. Based upon a statistical analysis performed by Professor Benjamin Highton at the University of California at Davis for this report, we estimate that if the attackers shut down three machines in a single polling place, the long lines created by the bottleneck would keep 7.7% of voters from voting in every affected precinct.[62] This means that roughly 88 voters per affected polling place (or 7.7% of 1142) would decide not to vote because of the bottleneck.

But not all of these voters would be Jefferson voters. Even if all of the affected polling places favored Tom Jefferson by 9 to 1, the bottleneck would cause both candidates to lose some votes. Presumably, for every 9 Jefferson voters turned away, 1 Adams voter would also decide not to vote. This means that, if this attack were limited to polling places that heavily favored Tom Jefferson, the effect would be to cause a net loss of 70 votes for Tom Jefferson per polling place (Tom Jefferson would lose 79, or 90% of the votes lost in each affected polling place, but Johnny Adams would lose 9, or 10%).

Based upon this information, we can determine how many polling places would need to be targeted:

number of
polling places targeted = (total votes targeted) /
(net number of votes lost by creating bottleneck)

or, in actual numbers:

number of
polling places targeted = 103,781 / 70 = 1,483

This represents more than one-third of all polling places in Pennasota.[63] It is doubtful that one-third of all polling places in Pennasota would be skewed so heavily toward Jefferson. Professor Henry Brady of the University of California

at Berkeley recently performed an analysis of election results in heavily Democratic Broward and Palm Beach counties in the 2000 election. *See* Appendix I. Even in those counties, only 21.4% and 14.8% of precincts, respectively, reported more than 80% of voters voting for Al Gore; furthermore, only 10.3% and 6.5% (respectively) reported 90% or more voting for Gore.

But even if we were to presume that there were enough polling places to allow this attack to work, there are other problems. First, the attack would probably be exposed: if thousands of machines were reported to have malfunctioned in polling places, but only where Jefferson was heavily favored, someone would probably notice the pattern.

Moreover, the number of informed participants necessary to carry out this attack makes it, in all likelihood, unworkable. The attack would need over 20,000 participants: 5 attackers per machine × 3 machines per polling place × 1,483 polling places.

All other "retail" attacks in the catalog require many hundreds or thousands of co-conspirators. For the reasons already discussed, we believe this makes these attacks very difficult to execute successfully in a statewide election.

In contrast, "wholesale" attacks allow less than a handful of individuals to affect many votes – enough, in some cases, to change the result of our hypothetical governor's race. The least difficult of these wholesale attacks are attacks that use Software Attack Programs. The following section discusses the feasibility of these attacks, which we have identified as the "least difficult" set of attacks against all three voting systems.

SOFTWARE ATTACKS ON VOTING MACHINES[64]

A Trojan Horse is a destructive program that masquerades as a benign program.

As already discussed, *supra* p. 6, attacks on elections and voting systems have a long history in the United States. One of the primary conclusions of this report is that, with the new primacy of electronic voting systems, attacks using Trojan horses or other Software Attack Programs provide the least difficult means to affect the outcome of a statewide election using as few informed participants as possible.

This conclusion runs counter to an assertion that many skeptics of these attacks have made, namely that it is not realistic to believe that attackers would be sophisticated enough to create and successfully implement a Software Attack Program that can work without detection. After careful study of this issue, we have concluded that, while operationally difficult, these threats are credible.

HISTORY OF SOFTWARE-BASED ATTACKS

Those skeptical of software attacks on voting machines point to the fact that, up to this point, there is no evidence that a software attack has been successfully carried out against a voting system in the United States. However, the best piece of evidence that such threats should be taken seriously is that, in the last several years, there have been increasingly sophisticated attacks on non-voting computer systems.

Among the targets have been:

- US government systems, including those containing classified data;[65]
- Financial systems, including attacks that gained perpetrators large sums of money;[66]
- Content protection systems intended to stand up to extensive external attack;[67]
- Special-purpose cryptographic devices intended to be resistant to both software and physical attack;[68]
- Cryptographic and security software, designed specifically to resist attack,[69] and
- Attacks on gambling machines, which are subject to strict industry and government regulation.[70]

We learn of more attacks on non-voting systems all the time. But, even with this increased knowledge, we have probably only learned of a small fraction of the attacks that have occurred. For each high-profile case of eavesdropping on cell phones or review of e-mails or pager messages, there are, in all probability, many

cases where the attacker's actions remain unknown to the public at large. For every case where financial data is tampered with and the theft is discovered and reported, there are certainly cases where it is never detected, or is detected but never reported.

Many existing attackers have *already shown themselves* to be sophisticated enough to carry out these types of attacks.

In addition to the attacks already listed, we also have seen the rise of sophisticated attacks on widely-used computer systems (desktop PCs) for a variety of criminal purposes that allow criminals to make money:

- Activities/methods like phishing (spam intended to get users to disclose private data that allow an attacker to steal their money) and pharming (exploitation of DNS[71] to redirect legitimate web traffic to illegitimate sites to obtain private data) continue to grow.[72]

Domain Name System (DNS) is a distributed database that stores mappings of Internet Protocol addresses and host names to facilitate user-friendly web browsing.

- Extortion against some computer sites continues, with an attacker threatening to shut down the site via a distributed denial-of-services (DDOS) attack, or the posting of confidential information, unless she is paid off.[73]

- Large networks of "bots" – innocent users' computers that have been taken over by an attacker for use in the kinds of attacks already referenced, are bought, sold and rented.[74]

The sophistication of these attacks undermines the argument that attackers "wouldn't be smart enough" to carry out a software attack on voting systems. Many existing attackers have *already shown themselves* to be sophisticated enough to carry out these types of attacks. In fact, given the stakes involved in changing the outcome of a statewide or national election, there is good reason to believe that many who would have an interest in affecting such outcomes are far more sophisticated than recent attackers who have hacked or violated well-protected government and private industry systems.

Still, there are several reasons to be skeptical of software-based attacks, and the rest of this section attempts to address the main challenges an attacker using this method of attack would face:

1. Overcoming Vendor Motivation. The vendor has an economic interest in preventing attackers from infiltrating their machines with Software Attack Programs.

2. Finding an Insertion Opportunity. An attacker would have to gain access to a place that would allow her to insert the Software Attack Program in the machine.

3. Obtaining Technical Knowledge. An attacker would have to know enough to develop a Software Attack Program that can function successfully in a voting terminal.

4. Obtaining Election Knowledge. An attacker may need to know a lot about the ballots and voting patterns of different precincts to create a Software Attack Program that works and does not create undue suspicion.

5. Changing Votes. Once an attacker has sufficient knowledge about the ballots and election, she would need to create a program that can change vote totals or otherwise affect the outcome of an election.

6. Eluding Inspection. An attack would have to avoid detection during inspection.

7. Eluding Testing and Detection Before, During, and After the Election. An attacker would have to avoid detection during testing.

8. Avoiding Detection After Polls Close. Even after an attack has successfully changed the electronic record of votes, an attacker would still need to ensure that it is not discovered later.

We review each of these barriers to successful software-based attacks in turn.

VENDOR DESIRE TO PREVENT SOFTWARE ATTACK PROGRAMS

Voting machine vendors have many reasons to want to protect their systems from attack. The most obvious reason is economic: a system that is shown to be vulnerable to attack is less likely to be purchased.

Unfortunately, the fact that vendors have incentives to create secure systems does not mean that their systems are as secure as they should be. The CERT (Computer Emergency Readiness Team) Coordination Center, a federally funded research and development center operated by Carnegie Mellon University, reported nearly 6,000 computer system vulnerabilities in 2005 alone. This included vulnerabilities in two operating systems frequently used on voting machines: 2,328 vulnerabilities on the Linux and Unix operating systems and 812 vulnerabilities in Microsoft Windows operating systems.[75] Many of these vulnerabilities leave machines open to "viruses and other programs that could overtake" them.[76]

Moreover, it is not clear that vendors are doing everything they can to safeguard their systems from attack. As noted in a recent Government Accountability Office report on electronic voting systems, several state election officials, computer security and election experts have criticized vendors for, among other things, their (1) personnel security policies, questioning whether they conduct sufficient background checks on programmers and systems developers, and (2) internal security policies, questioning whether such policies have been implemented and adhered to during software development. [77]

Even assuming that vendors adhere to the strictest personnel and security policies, it is still possible that they would hire employees who abuse their positions to place corrupt software into voting machines. A single, ill-intentioned employee could cause tremendous damage. This is illustrated by the case of Ron Harris, "a mid-level computer technician" for Nevada's Gaming Control Board.[78] Mr. Harris hid a Software Attack Program in dozens of video-poker and slot machines in the early 1990s. The attack program allowed accomplices to trigger jackpots by placing bets in a specific order. Mr. Harris was eventually caught because he became too brazen: by the mid-1990s, he began using an attack program against the gaming machines based on the card game "Keno." When his accomplice attempted to redeem a $100,000 jackpot, officials became suspicious and she was ultimately investigated and caught.[79]

A single, ill-intentioned employee could cause tremendous damage.

In any event, as demonstrated below, an attacker need not be employed at a vendor to insert an attack program into voting machines. She can choose several points to insert her attack, and many of them do not originate at the vendor.

INSERTING THE ATTACK PROGRAM

In this subsection, we look at some of the points where an attacker could insert her attack program. As illustrated by the chart on the next page, the attack program could be inserted while the machine is still in the hands of the vendor, after it has been purchased, and even on Election Day. Insertion into (1) Commercial Off The Shelf (COTS) software used on all voting machines, (2) COTS patches[80] and updates, and (3) ballot definition files,[81] may be particularly attractive because these are not currently subject to inspection by independent testers. Given their size and complexity, it is hard to imagine that a thorough review of them would be practical, even if the COTS vendors were willing to provide access to their source code for inspection.

A patch is a small piece of software designed to update or fix problems in a computer program.

Ballot definition files tell the voting machine how to interpret, display and record the voter's selections

POINTS OF ATTACK: COTS AND VENDOR SOFTWARE

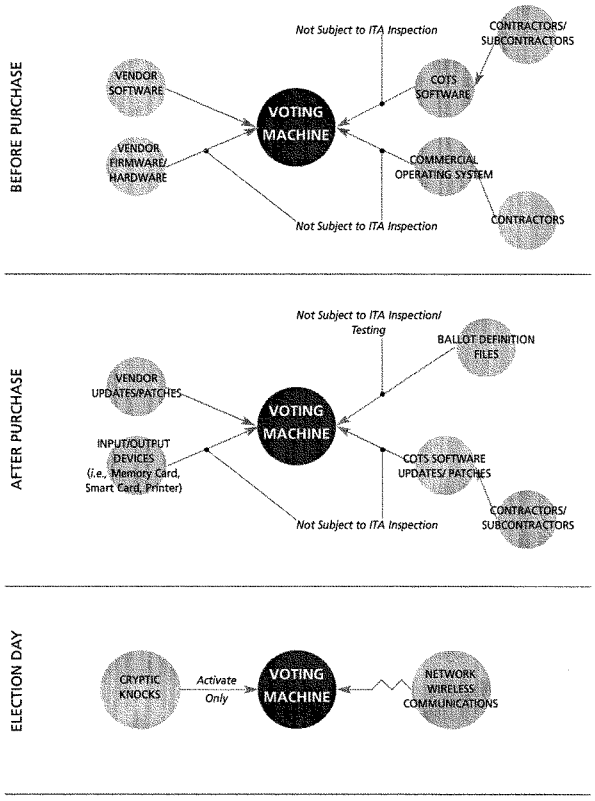
The process for developing voting system software is not dramatically different from the development of any other type of software or operating systems. Vendors develop a set of requirements for their machines; a team of programmers is subsequently assembled to apply those requirements by developing new code, and then integrating the new code with old code and COTS software; after the new code is written and integrated, a separate team of employees test the machines; when the testers find bugs, they send the new software back to the programmers (which may include new team members) to develop patches for the bugs.

There are a number of opportunities to insert a Software Attack Program during this process:[82]

- The attack program could be part of COTS software that was purchased for use on the voting system. The current voting systems standards exempt unaltered COTS software from inspection by an Independent Testing Authority.[83]
- The attack program could be written into the vendor code by a team member at the vendor.

FIGURE 6

SOFTWARE ATTACK PROGRAM: POINTS OF ENTRY



A cryptic knock is an action taken by a user of the machine that triggers a response by the embedded attack program. The cryptic knock could come in different forms depending on the attack program: voting for a write-in candidate, tapping a specific spot on the touch-screen, a communication via wireless network, etc.

- The attack program could be hidden within the operating system using rootkit-like techniques, or perhaps a commercial rootkit for the underlying operating system. [84]

- The attack program could be written into one of the patches that is developed after the vendor's testers find bugs.

- The attack program could be written by someone at the vendor after it has passed the vendor's testing.

Anyone with access to the voting system software before it has been installed on the voting machines may install an attack program.

A rootkit is a set of software tools used by an intruder to maintain access to a computer system without the user's knowledge.

It is worth noting that even tampering with the software in the *initial voting system is not limited to programmers working for the voting system vendor.* COTS software writers, who may themselves be contractors or subcontractors of the original company that sold the COTS software to voting systems vendors, are in a very good position to insert an attack program.

Further, anyone with access to the voting system software before it has been installed on the voting machines may install an attack program. This could include people with access to the software during development, storage, or testing.

POINTS OF ATTACK: SOFTWARE PATCHES AND UPDATES

COTS software is often supplemented by patches and updates that can add features, extend the software's capabilities (*e.g.*, by supporting more assistive technology or a larger set of screen characters for alternate-language voting) or fix problems discovered after the software was sold. This is an obvious attack point. The attack program may be inserted by someone working for the COTS software vendor, or by someone working at the voting system vendor, or by the election official handling the installation of patches and updates. The patch or update can be installed before or after the voting machine has left the vendor.

POINTS OF ATTACK: CONFIGURATION FILES AND ELECTION DEFINITIONS

As discussed, *supra* endnote 81, ballot definition files allow the machine to (1) display the races and candidates in a given election, and (2) record the votes cast. Ballot definition files cannot be created until shortly before an election, when all of the relevant candidates and races for a particular jurisdiction are known. An attacker could take over the machine by inserting improperly formed files at the time of Ballot Definition Configuration. Two separate reports have demonstrated that it may be possible to alter the ballot definition files on certain DREs so that the votes shown for one candidate are recorded and counted for another.[85] The Task Force knows of no reason why PCOS systems would not be similarly vulnerable to such an attack.

Ballot definition files are not subject to testing by Independent Testing Authorities

Two separate reports have demonstrated that it may be possible to alter the ballot definition files on certain DREs so that the votes shown for one candidate are recorded and counted for another. The Task Force knows of no reason why PCOS systems would not be similarly vulnerable to such an attack.

and cannot be because they are developed for specific jurisdictions and elections, after certification of a voting system is complete.[86]

POINTS OF ATTACK: NETWORK COMMUNICATION

As will be discussed in greater detail, *infra* pp. 85–86, some voting systems use wireless or wired network connections. If there is a vulnerability in the configuration of the voting machine (again, by design or error), this can allow an attacker to insert an attack program via the wireless connection.

POINTS OF ATTACK: DEVICE INPUT/OUTPUT[87]

Some voting systems involve the use of an external device such as a memory card, printer, or smart card. In some cases, the ability to use these devices to change votes has been demonstrated in the laboratory. For example, Harri Hursti, a member of the Task Force, has demonstrated that memory cards (which generally contain, among other things, the ballot definition files) can be used to create false vote totals on a particular brand of PCOS, and conceal this manipulation in reports to election officials generated by the scanners.[88] This was recently demonstrated again in a test performed by election officials in Leon County, Florida.[89] Several computer security experts who have reviewed other PCOS systems believe that they may be vulnerable to similar attacks.[90]

DREs have also been shown to be vulnerable to attacks from input devices. In a "Red Team" exercise[91] for the State of Maryland in January 2004, RABA Technologies, LLC demonstrated that smart cards (which are used as both supervisor and voter access cards) on one model of DRE could be manipulated to allow a voter to vote multiple times.

TECHNICAL KNOWLEDGE

Just because there are opportunities to insert a Software Attack Program does not mean that an attacker would have the knowledge to create a program that works. It is not difficult to understand how hackers could gain enough knowledge to create attack programs that could infiltrate common operating systems on personal computers: the operating systems and personal computers are publicly available commercial products. A hacker could buy these products and spend months or years learning about them before creating an effective attack program.

How would an attacker gain enough knowledge about voting systems to create an attack program that worked? These are not systems that general members of the public can buy.

We believe there are a number of ways an attacker could gain this knowledge. First, she might have worked for (or received assistance from someone who worked for) one of the voting system vendors. Similarly, she could have worked

for one of the independent testing authorities or state qualification examiners.

Alternatively, the attacker could hack into vendor or testing authority networks. This could allow her to gain important knowledge about a voting machine's software and specifications.

Finally, an attacker could steal or "borrow" a voting machine. Access to voting machines will be very important to an attacker as she develops her Software Attack Program; this will not necessarily be an overwhelming obstacle. Machines are often left in warehouses and polling places for months in between elections. Responses to our security surveys showed that there are many points where physical security for voting machines is surprisingly lax: about half of the counties responding to the security survey stated that they did not place tamper-evident seals on machines during the months the machines were in storage; several counties stated that they did not take inventory of voting machines in between elections; in one county, voting machines were placed under a blanket in the back of an office cubicle when not in use.[92] Hackers have repeatedly shown their ability to decipher software and develop attack programs by "reverse engineering" their target machines; there is no reason to believe they could not apply these skills to voting machines.[93]

Responses to our security surveys showed that there are many points where physical security for voting machines is surprisingly lax.

ELECTION KNOWLEDGE

An attacker could be required to insert the Software Attack Program before all facts about the election are known. Many points of insertion discussed above (*supra* pp. 33–36) would require the attacker to create an attack program before she could possibly know which candidates were running or where various races would be placed on ballots. Different jurisdictions could decide to place that same race in different positions on the ballot (*i.e.*, as the third race as opposed to the fourth).

ATTACKING THE TOP OF THE TICKET

We believe this problem could be overcome, particularly where the attacker sought to shift votes at the "top" of the ticket – as would be the case in an attempt to affect the governor's race in Pennasota in 2007. Here, in a software update or patch that is sent before a particular election, the attacker could merely ask the machine to switch one or two votes in the first race in the next election. Since the Federalists and the Democratic-Republicans are the two main parties in Pennasota, the attacker would know that their candidates for governor would be listed in the first and second columns in the governor's race. Even if the attacker is not certain whom the Federalists or Democratic-Republicans are going to select as candidates at the time when she inserts the attack program, she could still create a successful program by instructing the machine to switch a certain number of votes in the first (governor's) race from the Democratic-Republicans (column "2") to the Federalists (column "1").

Moreover, we have assumed that our attacker is smart enough to avoid switching so many votes that her attack would arouse suspicion. By switching 7.5% or fewer votes per machine, our attacker need not be particular about which machine she attacks. She could create a program that only activates on every fourth or fifth machine.

PARAMETERIZATION

It is possible that our attacker would be more cautious: perhaps she would limit her attack to certain counties or precincts. Perhaps in some jurisdictions the governor's race won't be listed as the first race. Or perhaps her opportunity to insert the attack program came a year before the governor's race, when she wasn't sure who the candidates would be and whether she would want to attack the election.

In such cases, the attacker could "parameterize" her attack. Under this scenario, the attacker would create an attack program and insert it in the original software, or software updates. The attack program would not specify which race to attack or how. Instead, it would wait for certain commands later; these commands would tell it which votes to switch.

These commands could come from many sources, and could be difficult for anyone other than the attacker to find. For instance, the commands could come from the ballot definition file.[94] The original attack program could provide that if there is an extra space after the last name of the second candidate for a particular race in a ballot definition file, five votes in that race should be switched from the second column to the first. By waiting to provide these commands until the ballot definition files are created, the attackers could affect a race with great specificity – instructing the attack program to hit specific precincts in specific ways.

Of course, this is a more difficult attack: it requires more steps and more informed participants (both the original programmer and the person to insert the commands in the ballot definition file). In the specific example we have provided, it would also require someone with insider access to the ballot definition files.

But this type of attack would be attractive because it would give the attacker a great deal of flexibility. Moreover, the commands could come from sources other than the ballot definition files. If the voting machines have wireless components, the attacker could activate her attack by sending commands over a wireless PDA[95] or laptop. Or she could send these commands through a Cryptic Knock[96] during, for instance, voting or Logic and Accuracy testing.[97] For example, an insider responsible for developing the Logic and Accuracy scripts could have all the testers type in a write-in candidate for the ostensible purpose of ensuring that the write-in function is working. The spelling of the name of that write-in candidate could encode information about what races and ballot items should be the target of the attack. Testers following the script would unknowingly aid the attack.

CREATING AN ATTACK PROGRAM THAT CHANGES VOTES

Even if the attacker possessed sufficient knowledge about voting systems and specific elections before she inserted her attack program, she would need to figure out a way to create a tampering program that alters votes.[98] Without getting into the fine details, this subsection will summarize a number of methods to accomplish this goal.

CHANGING SYSTEM SETTINGS OR CONFIGURATION FILES

Configuration Files are files that are created to organize and arrange the system settings for voting machines. The system settings control the operation of the voting machine: for instance, setting parameters for what kind of mark should count as a vote on the PCOS ballot, instructing the PCOS scanner to reject ballots that contain overvotes, setting parameters for dividing a DRE screen when there are multiple candidates in the same race, or providing a time limit for voters to cast their votes on DREs.

An attack program that altered the system settings or Configuration Files could be buried in a Driver or program that is only run when the voting has started, or work off of the voting machine clock, to ensure that it is triggered at a certain time on Election Day. Among the attacker's many options within this class of attack are:

- Swap contestants in the ballot definition or other files, so that, for instance, a vote for Tom Jefferson is counted as one for Johnny Adams (and vice versa). This is an attack that was described in the RABA Technologies report on an intrusion performed for the state of Maryland.[99]

- Alter Configuration Files or system settings for the touch-screen or other user interface device, to cause the machine to cause differential error rates for one side. For instance, if our attacker knew that voters for Tom Jefferson were more likely to overvote or undervote the first time they filled out their ballots, she could install a software attack that shut off the overvote/undervote protection in several PCOS scanners – *see infra* p. 81 for a discussion of this attack.

- Alter Configuration Files or system settings to make it easier to skip a contest or misrecord a vote accidentally (*e.g.*, by increasing or decreasing touch-screen sensitivity or misaligning the touch-screen).

- Alter Configuration Files or system settings to change the behavior of the voting machine in special cases, such as when voters flee (for instance, recording a vote for Johnny Adams when a voter leaves the booth without instructing the machine to accept her ballot).

The attack that introduces biased errors into the voter's interaction with the voting system is especially useful for attacking DRE w/VVPT and PCOS systems since the attacked behavior, if detected, is indistinguishable from user error.

There are at least two potential operational difficulties an attacker would have to overcome once she inserts this type of attack program: (1) she would need to control the trigger time of the attack so as to avoid detection during testing; and (2) she would want to make sure that the changes made are not entered into the Event Logs, in case they are checked after the polls have closed. Ways of overcoming these challenges are discussed *infra* pp. 42–44 and 44–46.

ACTIVE TAMPERING WITH USER INTERACTION OR RECORDING OF VOTES

In this type of attack, the attack program triggers during voting and interferes in the interaction between the voter and the voting system. For example, the attack program may:

- Tamper with the voter interaction to introduce an occasional "error" in favor of one contestant (and hope that the voter does not notice). This is the "Biased Error" attack.

- Tamper with the voter interaction both at the time the voter enters his vote and on the verification screen, so that the voter sees consistent feedback that indicates his vote was cast correctly, but the rest of the voting machines software sees the changed vote.

- Tamper with the electronic record written after the verification screen is accepted by the voter – *e.g.*, by intercepting and altering the message containing results before they are written in the machine's electronic record, or any time before end-of-election-day tapes (which contain the printed vote totals) are produced and data are provided to election officials.

This class of attack seems to raise few operational difficulties once the attack program is in place. The attack that introduces biased errors into the voter's interaction with the voting system is especially useful for attacking DRE w/VVPT and PCOS systems where the paper record is printed or filled in by the voting machines being attacked, since the attacked behavior, if detected, is indistinguishable from user error. However, the attack program could improve its rate of successfully changed votes, and minimize its chances of detection, by choosing voters who are unlikely to check their paper records carefully. Thus, voters using assistive technology are likely targets.

TAMPERING WITH ELECTRONIC MEMORY AFTER THE FACT

An alternative approach is to change votes in electronic memory after voting has ended for the day, but before the totals are displayed locally or sent to the county tally server.

In this case, the attack program need only be activated after voting is complete.

This allows the attack program considerable flexibility, as it can decide whether to tamper with votes at all, based on totals in the machine. For instance, the Software Attack Program could be programmed to switch ten votes from Tom Jefferson to Johnny Adams, only if Johnny Adams has more than 90 votes on the machine.

It can also allow the attack program to avoid getting caught during pre-election testing. By programming the attack program to activate only after voting has ceased on Election Day (and the program should be able to do this by accessing the voting machine's internal clock), the attack program would elude all attempts to catch it through earlier testing. Similarly, by only triggering after, for instance, 100 votes have been cast within twelve hours, the attack program can probably elude pre-election testing; most pre-election testing involves the casting of far fewer votes. *See* Appendix E.

This type of attack must overcome some interesting operational difficulties; we do not believe that any of them are insurmountable with respect to any of the systems we have reviewed:

- Some voting machines store electronic records in several locations; the attack program would have to change them all.

- The attack program must either (1) avoid leaving entries of attack in the Event or Audit Logs, or (2) create its own Audit Logs after the attack (however, the necessity of doing either of these things is dependent upon how the machine logs its own actions: if the machine would show only that it accessed a file, these are unlikely to be problems for the attack program; if each record altered yields a log entry, this requires tampering with the event log to avoid detection).

- Depending upon details of the file access required, the attack program may face some time constraints in making the desired number of changes. Given the fact that we have assumed no more than 7.5% of votes would be switched in any one polling place or 15% on any machine, this may not be a great problem. There is likely to be a reasonable span of time between the closing of polls and the display and transmission of results.

Attacks installed at certain points may not be subject to any inspection.

ELUDING INDEPENDENT TESTING AUTHORITY INSPECTIONS[100]

How does an attacker ensure that an attack program she has inserted would not be caught by inspections[101] done at the vendor, or during an Independent Testing Authority inspection of software code?

Part of the answer depends upon where the attack program is installed. Attacks installed at certain points (such as attacks written into vendor software code) are likely to be subject to multiple inspections; attacks installed at other points (such as attacks installed in COTS software, ballot definition files or replaceable media) may not be subject to any inspection.

CREATE DIFFERENT HUMAN-READABLE AND BINARY CODE[102]

A clever attacker could defeat inspection in a number of ways. Before detailing how this would be accomplished, a brief conceptual introduction is necessary: To develop a program, a programmer writes human-readable source code. Generally, before a computer can run this program, the source code must be converted into a binary code (made up of "0"s and "1"s) that the computer can read. This conversion is accomplished by use of a compiler.[103] Thus, each program has two forms: the human-readable source code and the compiled binary code.

A simple attack designed to elude inspection could be accomplished as follows: our attacker writes human-readable source code that contains an attack program (perhaps the program, among other things, instructs the machine to switch every 25th vote for the Democratic-Republicans to the Federalists). The attacker then uses a compiler to create a similarly malicious binary code to be read by the computer. After the malicious binary code has been created, the attacker replaces the malicious human-readable source code with a harmless version. When the vendor and Independent Testing Authority inspect the human-readable source code, they would not be able to detect the attack (and the binary code would be meaningless to any human inspector).

USE ATTACK COMPILER, LINKER, LOADER OR FIRMWARE

An obvious way for an ITA to pre-empt this attack would be to require vendors to provide the human-readable source code, and to run the human-readable source code through the ITA's compiler. The ITA could then compare its compiled version of the code with the compiled code provided by the vendor (*i.e.*, did all the "0"s and "1"s in both versions of the code match up?).

But what if, instead of inserting the attack into the vendor's source code, our attacker inserted an attack into the compiler (which is generally a standard software program created by a non-voting system software vendor)? Under these circumstances, the compiler could take harmless human-readable source code and

turn it into malicious binary code without any inspector being the wiser. As a compiler is generally COTS software, it would not be inspected by the ITAs.

In any event, the attacker could hide the attack program in the compiler by adding one level of complexity to her attack: make the compiler misread not only the seemingly innocuous vendor source code (which would be converted into malicious binary code), but also the seemingly innocuous compiler source code (which would also be converted into malicious binary code, for the purpose of misreading the vendor source code). In other words, the attacker can hide the attack program in the same way that she might hide an attack program in other software: change the human-readable compiler source code so that it does not reveal the attack. When the compiler "compiles itself" (*i.e.*, turning the human-readable source code for the compiler into computer readable binary code) it creates a binary code that is malicious, but cannot be detected by human inspectors.

The compiler is not our attacker's only opportunity to convert innocuous human-readable source code into an attack program. What is known as a "linker" links the various binary code programs together so that the voting machine can function as a single system. Here again, the linker can be used to modify the binary code so that it functions as an attack program.

Additionally, the attacker can use the "loader," the program on each voting machine's operating system that loads software from the disk drive onto the machine's main memory, to alter code for a malicious purpose.[104]

Finally, if our attacker is a programmer employed at the vendor, she can create or alter firmware[105] that is embedded in the voting machines' motherboard, disk drives, video card or other device controllers to alter seemingly harmless code to create a malicious program. Like COTS software, firmware is not subject to ITA inspection.

AVOIDING INSPECTION ALTOGETHER

An attacker could also insert her program in places not subject to inspection.

As already noted, the current Voluntary Voting Systems Guidelines exempts unaltered COTS software from testing, and original COTS code is not currently inspected by the ITAs.[106] This makes it more difficult to catch subtle bugs in either COTS software that is part of the original voting system, or COTS software patches and updates (assuming that new testing is done when such patches and updates are required).

Moreover, attacks inserted through ballot definition, via wireless communication, or through device input (*i.e.*, memory cards, printers, audibility files) would occur after the machine has been tested by the ITA and would thus avoid such testing altogether.

Moreover, we have serious concerns about the ability of current Independent Testing Authority inspections and tests to catch even Software Attack Programs and bugs in original voting systems software. While ITA tests may filter out obvious attack behavior, intentional, subtle bugs or subtle attack behavior (*e.g.*, triggering the attack behavior only after complicated interaction with a user unlikely to be replicated in a testing lab, or only when the clock tells the Attack Program that it is Election Day) may remain unnoticed in the testing lab review. As noted in the GAO report, these and other concerns about relying on ITA testing have been echoed by many security and testing experts, including ITA officials.[107]

AVOIDING DETECTION DURING TESTING

Even after an attack program has been successfully installed and passed inspection, it would still need to get through testing. Tampered software must avoid detection during testing by vendors, testing authorities and election officials. With the exception of Parallel Testing (which is regularly performed statewide only in California, Maryland, Washington), all of this testing is done prior to voting on Election Day.[108]

There are a number of techniques that could be used to ensure that testing does not detect the attack program.

- The attack program could note the time and date on the voting machine's clock, and only trigger when the time and date are consistent with an election. This method could, by itself, prevent detection during vendor testing, Logic and Accuracy Testing and Acceptance Testing, but not during Parallel Testing.

- The attack program could observe behavior that is consistent with a test (as opposed to actual voter behavior). For example, if Logic and Accuracy Testing is known never to take more than four hours, the attack program could wait until the seventh hour to trigger. (Note that the attack becomes more difficult if the protocol for testing varies from election to election).

- The attack program could activate only when it receives some communication from the attacker or her confederates. For example, some specific pattern of interaction, a Cryptic Knock, between the voter or election official and the voting machine may be used to trigger the attack behavior.

AVOIDING DETECTION AFTER THE POLLS HAVE CLOSED

In many cases, the most effective way to tamper with an election without detection would be to change votes that have actually been cast; this way, there would be no unusual discrepancy between the poll books (which record the number of voters who sign in) and vote totals reported by the machines.[109] In the case of a DRE

system, changing votes electronically changes all official records of the voter's choice, so this kind of attack cannot be directly detected by comparing the electronic totals with other records. In the case of other voting systems, such as DRE w/VVPT or PCOS, the attacker must also tamper with the paper records, or prevent their being cross-checked against the electronic records, *assuming that there is some policy in place that requires jurisdictions to check paper records against the electronic totals.*

In the case of a DRE system, changing votes electronically changes all official records of the voter's choice, so this kind of attack cannot be directly detected by comparing the electronic totals with other records.

DECIDING HOW MANY VOTES TO CHANGE

An attack could be detected if there were a very strong discrepancy between informal numbers (polling data, or official results in comparable precincts or counties) and reported election results. There are at least a couple of ways that an attack program could minimize suspicion from this kind of evidence:

- Where possible, the attack program on the voting machines would change a fixed portion of the votes (for instance, in the attack scenarios we have developed, we have assumed that no more than 7.5% of votes in any single polling place would be switched), rather than simply reporting a pre-ordained result. This avoids the situation where, for instance, a recently indicted candidate mysteriously wins a few precincts by large margins, while losing badly in all others, raising suspicion that there was an attack. It also prevents a situation where a candidate wins 80–90% of the vote in one polling place, while losing badly in all other demographically similar polling places.

- The attack program might also detect when the tampering is hopeless (*e.g.*, when the election appears so one-sided that the benefit of improving the favored candidate's outcome is outweighed by the cost of increased chance of detection from implausible results). In that case, it would refrain from any tampering at all, since this would risk detection without any corresponding chance of success.

AVOIDING EVENT AND AUDIT LOGS

Tampered software must not leave telltale signs of the attack in any Event or Audit Logs.[110] There are a number of ways the attack program could accomplish this goal, depending upon the nature of the attack program and the software it targets:

- Tampered user-interface software could display the wrong information to the voter (meaning the voter believes his vote has been recorded accurately), while recording the attack program choice in all other system events. In this case, there would be no trace of the attack in the event log.[111]

- Tampered Driver software for storage devices or tampered BIOS[112] could alter what is written to the storage devices.

BIOS ("basic input/output system") is the built-in software that determines what a computer can do without accessing programs from a disk.

- A tampered operating system or other high-privilege-level software could tamper with the logs after entries are made, avoiding record of such an attack in the logs.[113]

- A tampered operating system or other software could provide a different log to the outside world than the one stored internally, if the log is not stored on removable media.

COORDINATING WITH PAPER RECORD ATTACKS[114]

When the attacker must also tamper with paper records (*i.e.*, in the case of PCOS and DRE w/VVPT systems), she would likely need to prepare replacement paper records before the voting is completed.[115]

This coordination task could be solved in a number of ways:

- The attacker could wait until the election is over, and then print the replacement paper records. This raises some logistical problems for the attacker, such as how to find out what the electronic records show, and print enough paper records once this information is learned and replace the paper.

- If the attacker is in contact with the voting machine during the voting process – for example over a wireless network or via an exposed infrared port – the attacker could print replacement paper records as the tampered records are produced on the voting machine.

- The attack program could have a predefined sequence of votes, which it produces electronically and which the attacker can print at any time.

- The attacker could communicate with the voting machine after voting has ended but before the votes have been displayed to poll workers or sent to the tabulation center. In this case, the attacker could tell the voting machine what totals to report and store. This could be done remotely (via wireless or exposed infrared port) or through some form of direct interaction with the machine (this would obviously require many conspirators if multiple machines were involved).

In all cases, the attacker would have the additional problem of replacing the original records with her created paper records. We discuss this issue *infra* pp. 71–75.[116]

CONCLUSIONS

Planting a Trojan Horse or other Software Attack Program, though operationally challenging, is something that a sophisticated attacker could do. An attacker could take advantage of several points of vulnerability to insert corrupt software. Many of these points of vulnerability are currently outside the testing and inspection regimen for voting systems. In any event, we are not confident that testing and inspection would find corrupt software even when that software is directly tested and inspected by an ITA.

Our attacker – who aims to move roughly 52,000 votes from the Democratic-Republicans to the Federalists in the gubernatorial race in Pennasota – need not know much about the particulars of the election or about local ballots to create an effective attack program, and thus could create her attack program at almost any time. To the extent she is concerned about the names of the candidates or particulars of local ballots, however, she could parameterize her attack by, for instance, inserting instructions into the ballot definition files or sending instructions over a wireless component, when she would have all the information she could want about local ballots.

There are a number of steps – such as inspecting machines to make sure that all wireless capabilities are disabled – that jurisdictions can take to make software attacks more difficult. Ultimately, however, this is a type of attack that should be taken seriously.

48

A software attack allows a single knowledgeable person (or, in some cases, small group of people) to reach hundreds or thousands of machines.

LEAST DIFFICULT ATTACKS APPLIED AGAINST EACH SYSTEM

As already discussed, in a close statewide election like the Pennasota governor's election, "retail" attacks, or attacks on individual polling places, would not likely affect enough votes to change the outcome. By contrast, the less difficult attacks are centralized attacks: these would occur against the entire voting system and allow an attacker to target many votes with few informed participants.

Least difficult among these less difficult attacks would be attacks that use Software Attack Programs. The reason is relatively straightforward: a software attack allows a single knowledgeable person (or, in some cases, small group of people) to reach hundreds or thousands of machines. For instance, software updates and patches are often sent to jurisdictions throughout a state.[117] Similarly, replaceable media such as memory cards and ballot definition files are generally programmed at the county level (or at the vendor) and sent to every polling place in the county.

These attacks have other benefits: unlike retail denial-of-service attacks, or manual shut off of machine functions, they could provide an attacker's favored candidate with a relatively certain benefit (*i.e.,* addition of x number of votes per machine attacked). And if installed in a clever way, these attacks have a good chance of eluding the standard inspection and testing regimens currently in place.

Below, we look at examples of these least difficult attacks against each system: how they would work, how many informed participants would be needed, how they might avoid detection, and how they could swing a statewide election. In addition, we evaluate the effectiveness of each of the three sets of countermeasures against them.

ATTACKS AGAINST DRES WITHOUT VVPT

The Task Force has identified over thirty-five (35) potential attacks against DREs without VVPT.[118] All of the least difficult attacks against DREs without VVPT involve inserting Software Attack Programs into the DREs. In this section, we will examine an example of this least difficult attack and how much more "expensive" such attacks are made by the "Basic Set" and "Parallel Testing Set" of countermeasures. *We cannot examine the "Automatic Routine Audit Set" of countermeasures against these attacks, because DREs do not have a voter-verified paper trail to allow auditing to occur.*

We are also particularly concerned about attacks that are made easier by use of wireless networks. This set of attacks will be examined here under "Prevention of Wireless Communications," *infra* pp. 85–86.

REPRESENTATIVE "LEAST DIFFICULT" ATTACK: TROJAN HORSE INSERTED INTO OPERATING SYSTEM (DRE ATTACK NUMBER 4)

As already discussed, there are several potential points of entry for a Software Attack Program. We could have chosen any number of Software Attack Programs in our DRE Attack Catalog. We have chosen Attack Number 4, "Trojan Horse Inserted into Operating System," because it is representative of these attacks and easy to explain.

As already discussed, a "Trojan Horse" is a type of Software Attack Program that masquerades as a benign program component. Unlike viruses, Trojan Horses do not replicate themselves.

DESCRIPTION OF POTENTIAL ATTACK

Here is how this representative attack works:[119]

- A third-party software company supplies a publicly available operating system for DREs.[120]

- As already noted, the Trojan Horse could be inserted by any number of people: a programmer working for the voting system vendor, the operating system vendor, or an employee of a company that contracts with the software company that creates the operating software.[121] The Trojan Horse could also be inserted in an operating system update or patch that would be inserted on any voting machine that ran on this operating system.[122]

- The attacker could change the human-readable source code for the operating system, to ensure that anyone who decided to inspect the code would not find the Trojan Horse. In any event, the operating system is COTS software, so it is unlikely to be reviewed by the vendor, or inspected by the ITA.

- The Trojan Horse is coordinated with the voting machine's internal clock and set to activate after ITA, Acceptance, and Logic and Accuracy Testing are complete (*e.g.*, the first Tuesday after the first Monday in November 2007, after 11 a.m.). This would prevent any detection during such testing.

- Among the many ways a Trojan Horse could ensure the misrecording of votes, it could:

    - Detect when a ballot is displayed, and reverse the order of the first two entries on the screen (so if the order should be, for example, Johnny Adams and Tom Jefferson, the displayed order is Tom Jefferson and Johnny Adams). In this scenario, the Trojan Horse would also check for the names on the review screen, and if either of the two names appeared, the other would be substituted and recorded.

- Alter votes in the electronic memory at the end of a full day of voting. This might be slightly more complicated, as it could require the Trojan Horse to change the electronic records in the many locations where vote totals are stored and avoid leaving entries in the Event and Audit Logs, or create new logs.

- Display information as the DRE is intended to (*i.e.*, ballot positions are not reversed and verification screens let voters believe their choices have been accurately recorded), but record the Trojan Horse's choice in all other system events.

- The Trojan Horse can attempt to ensure that no one would discover what it has done after the election is over, even if there are suspicions that machines were attacked:

  - It could tamper with the Event and Audit logs after the attack is complete, preventing the creation of a record of such an attack in the logs.

  - It could create and provide a new log to the outside world, different than that stored internally.

  - It could avoid the Event and Audit Logs altogether, by displaying the wrong information to the voter (*i.e.*, allowing the voter to believe his vote has been recorded correctly), while recording the Attack Program's choice in all other system events.

We estimate that with clever enough attackers, this attack could successfully be completed with just one person; this attack involves only one step: design and insertion of the Trojan Horse.[123] Obviously, it would be important for the designer of the Trojan Horse to understand the workings of the DRE she seeks to attack.[124] But once the Trojan Horse was successfully inserted, it would not require any further involvement or informed participants.

HOW THE ATTACK COULD SWING STATEWIDE ELECTION

In the race for governor of Pennasota, 3,459,379 votes would be cast, and the election would be decided by 80,257 votes (or 2.32%). We assume that the attacker would want to leave herself some margin of error, and therefore aim to (1) add 103,781 votes (or 3%) to Johnny Adams's total (or subtract the same from Tom Jefferson) or (2) switch 51,891 votes from Tom Jefferson to Johnny Adams.

As we assume that each DRE would record roughly 125 votes, we calculate that Pennasota would have approximately 27,675 DREs.[125] This would require the Software Attack Program *to switch fewer than 2 votes* per machine to change the outcome of this election and do so with a comfortable margin of victory.[126]

EFFECT OF BASIC SET OF COUNTERMEASURES

The Basic Set of Countermeasures that apply to DREs without VVPT are as follows:

- The model of DRE used in Pennasota has passed all relevant ITA inspections.
- Before and after Election Day, machines for each county are locked in a single room.
- Some form of tamper-evident seals are placed on machines before and after each election.
- The machines are transported to polling locations five to fifteen days before Election Day.
- Acceptance Testing is performed by every county at the time the machines are delivered from the vendor.
- Logic and Accuracy Testing is performed immediately prior to each election by the County Clerk.
- At the end of Election Day, vote tallies for each machine are totaled and compared with the number of persons who have signed the poll books.
- A copy of totals for each machine is posted at each polling place on election night and taken home by poll workers to check against what is posted publicly at election headquarters, on the web, in the papers, or elsewhere.

Given the small number of votes changed per machine, we do not believe that the altered machine totals alone would alert election officials or the public to the fact that election results had been changed.

As already explained, *supra* pp. 42–44, there is a good chance that the ITA (and, for that matter, the vendor) would not find the attack during its inspection of the code. First, the attacker could erase the Trojan Horse from the human-readable source code, on the chance that an inspector might review the operating system's source code carefully. In this case, only a careful forensic analysis of the machine could find the Trojan Horse. Second, because the operating system is COTS code, it is unlikely that the code for the operating system (and its updates and patches) would be inspected at all.[127] Third, if the Trojan Horse is part of an operating system update or patch, it may never even enter an ITA. The model would have already passed inspection; it is unlikely that local jurisdictions or the vendor would ask the ITA to conduct an entirely new test and inspection with a model that has the COTS patch or update installed.

Once the Trojan Horse was inserted, the physical security detailed in the Basic Set of Countermeasures would not be of any benefit.

Finally, the testing done in this set of countermeasures would not catch the attack. The Trojan Horse, by waiting until 11 a.m. on Election Day, would ensure that all testing is complete. Posting election night results at the polling place would not help either; these results would match county election totals. Unfortunately, neither set of numbers would match actual voter choice.

Based on this analysis, we have concluded that the Basic Set of Countermeasures would not require our attacker to add any more informed participants to complete her attack successfully.

EFFECT OF REGIMEN FOR PARALLEL TESTING

As already discussed, the Regimen for Parallel Testing involves selecting voting machines at random and testing them as realistically as possible during the period that votes are being cast. The object of this testing is to find any bug (whether deliberately or accidentally installed) that might be buried in the voting machine software and which could affect the ability of the voting machines to record votes accurately. Unlike other pre-election testing which is almost always done using a special "test mode" in the voting system, and thus might be subverted by a clever attacker relatively easily, Parallel Testing attempts to give no clues to the machine that it is being tested. Professional testers cast votes generated by a script for the full Election Day (this would allow the testers to find an attack that triggers, for example, after 11 a.m. on Election Day). If Parallel Testing is done as we suggest, these cast votes would simultaneously be recorded by a video camera. At the end of the day, election officials reconcile the votes cast on the tested machine with the results recorded by the machine. The video camera is a crucial element in the Regimen for Parallel Testing, because it allows officials to ensure that a contradiction between the machine record and the script is not the result of tester error.

The Trojan Horse attack is one of the attacks that Parallel Testing is intended to catch.[128] There should be no question that if properly implemented, Parallel Testing would make a Trojan Horse attack more difficult.

But how much more difficult, and in what way? In the following subsections, we assess the ways an attacker might subvert Parallel Testing and how difficult this subversion would be: this includes a review of the ways in which Parallel Testing may force an attacker to invest more time, money and technical savvy to implement a least difficult attack like DRE Attack Number 4 successfully. It also includes an assessment of the number of additional informed participants that would be needed to implement this attack when the Regimen for Parallel Testing Plus Basic Set of Countermeasures is in place.

We have identified two ways that an attacker might be able to subvert Parallel Testing, and thus still successfully implement DRE Attack Number 4. They are:

1. infiltrate the Parallel Testing teams; and

2. create an Attack Program that can recognize when it is being Parallel Tested and knows to shut off under such circumstances.

A state does not have to test a particularly large number of machines for Parallel Testing to catch a Trojan Horse that has been inserted for the purpose of changing the outcome of a statewide election.

As discussed in further detail below, in certain scenarios, an attacker could combine these two methods to subvert Parallel Testing.

Infiltrating the Parallel Testing Teams

Subverting Parallel Testing by simply infiltrating the Parallel Testing team would be extremely difficult. To have a reasonable chance of defeating Parallel Testing this way, the attacker would have to add approximately 100 informed participants to her conspiracy.[129]

As detailed in Appendix J, a state does not have to test a particularly large number of machines for Parallel Testing to catch a Trojan Horse that has been inserted for the purpose of changing the outcome of a statewide election. Assuming that 5% of all machines were attacked (and in Pennasota, we have determined that more than 7% would need to be attacked to swing a statewide election),[130] we calculate that it would be necessary to test only 58 machines to have a 95% chance of testing a machine that has a Trojan Horse.[131] As a reminder, under the Regimen for Parallel Testing Plus Basic Set of Countermeasures, every testing team would have a tester and observer.

If the attacker managed to infiltrate half of the teams of testers and observers and make them part of the attack conspiracy (for a total of 58 additional fully informed participants), there would still be a greater than 75% chance that uncorrupted parallel testers would test a machine that contained a Trojan Horse.[132]

To reduce the odds substantially, so that there would be just a 10% chance that Parallel Testing would catch the Trojan Horse, the attacker would need to involve all but two teams of testers (meaning she would need to involve over 100 parallel testers and observers in the conspiracy).[133]

Creating an Attack That Recognizes Testing

Rather than subvert Parallel Testing by infiltrating the Parallel Testing teams alone, an attacker's best bet would be to design an attack program that is capable of recognizing when it is being tested. How might a tampered program detect that a machine is being used by parallel testers, rather than by regular voters?

There are a number of possibilities:

1. Warning the Trojan Horse. Someone on the attack team may communicate with the Trojan Horse, for example by using a wireless data channel to deactivate the attack behavior when Parallel Testing is being conducted in a polling place, or to activate it when there is no Parallel Testing being conducted.

2. Detecting the Test Environment. The Trojan Horse may determine that the machine is being parallel tested by looking at details of interactions between the machine and the "voters" or the larger voting system. For instance, many machines require the insertion of a smartcard or memory token before they would record any votes. Usually, there are several tokens in one polling place, and any one of them can be used on any machine. This means that most machines would have to scan a number of tokens during an Election Day. A Trojan Horse might be able to detect that a machine is being parallel tested if the same smartcard or memory token is inserted in that same machine all day.[134]

3. Recognizing Vote Patterns. The Trojan Horse may determine that the machine is being parallel tested by looking at the pattern of votes cast. For example, if Parallel Testing is done with randomly selected votes on each ballot position, the attack program may quickly notice that the Green and Libertarian candidates are getting about as many votes as the Republican and Democrat.

4. Recognizing Usage Patterns. The Trojan Horse may determine that the machine is being parallel tested by looking at usage patterns such as number of votes, speed of voting, time between voters, commonness of unusual requests like alternative languages or assistive technology, *etc.* For example, if Parallel Testing is always done for exactly 100 votes, the attack program may simply leave the vote totals unchanged when it gets exactly 100 votes.[135] At the 101st vote, the Trojan Horse knows it is safe to activate, and can switch vote totals at that point.

The first two of these are largely solvable by technical measures, the second two are impossible to solve in principle; they lead to a kind of arms race between attackers and defenders, and it is unclear where the ultimate advantage would lie.

Warning the Trojan Horse

There are many ways for attackers to (1) warn a Trojan Horse that its machine is being parallel tested, so that the Trojan Horse suppresses any attack behavior, or (2) activate Trojan Horses only on machines the attackers know are not being tested.

First, parallel testers, voters or poll workers could manually "tell" machines whether they were being tested. The attackers could:

- Send voters to each machine to be used in the attack with some kind of Cryptic Knock such as a voting pattern extremely unlikely to occur in the Parallel Testing.

  There are problems with this attack: voters sent to these machines need not be fully informed about the attack; however, since they know the Cryptic Knock, they could inform the authorities about what they have been told to do, and thus could allow parallel testers to detect the attack. Also, this strategy would require involving over 1,000 registered voters if this attack is expected to swing the governor's race in Pennasota.[136]

- Have election officials turn on each machine for voting using some Cryptic Knock to activate the attack program.

  This still requires a great many insiders in the attack team, since some election official or poll worker must do this for each machine to be activated. We have estimated that a minimum of 606 polling stations would need to be attacked in our state to swing an election, so this would involve the participation of 606 pollworkers.[137]

- Have parallel testers warn machine being tested with a Cryptic Knock. Because it would only take a single tester to warn the machine (and because the Cryptic Knock could be an innocuous action, like tapping the screen three times in the upper left hand corner), it would be unnecessary to subvert the entire team; instead it would only be necessary to subvert one team member per testing team, for a total of 58 testers.

In some circumstances, attackers could also warn the machines remotely:

- If the voting machine is capable of receiving wireless data transmissions, *e.g.*, over a wireless network or through an infrared port, then a single member of the attack team with a wireless-enabled PDA could activate or deactivate an entire polling place full of machines' attack programs, after verifying that no Parallel Testing is being done nearby. Thus, in jurisdictions that use machines capable of receiving wireless transmissions, an attack with enough foresight and technical skills could subvert Parallel Testing by increasing her attack team size by a relatively small number (and none of these attackers would need to be insiders).[138]

- If the voting machine is networked with other voting machines, and the attack program is installed in all of them, then a voter or election official need only use her Cryptic Knock once per polling place to enable or disable the attack program on all connected machines.
- If the voting machine is connected over some network to a central server, an attacker could issue a centralized warning telling compromised machines at polling places that would be receiving Parallel Testing teams not to trigger

By removing any wireless channel by which voting machines can receive commands, the designer of a voting system can make Parallel Testing much more effective.

their attack behavior. This would require the attacker to (1) learn where Parallel Testing was occurring, and (2) find a method for infiltrating the network. Given the fact that jurisdictions in California are told which polling place would be tested at least a month in advance, it is plausible to imagine that this attack (against machines connected by a network to central servers) could be successful without dramatically increasing attack team size.

This discussion demonstrates the importance of closing machines off to remote communications: by removing any wireless channel by which voting machines can receive commands, the designer of a voting system can make Parallel Testing much more effective. Similarly, the effectiveness of Parallel Testing can be improved if the machines are never connected to one another during voting. Ideally, a voting machine would be completely isolated during the election and would print out or otherwise display its totals *before* being connected to any central server to send in its tallies.

Detecting the Test Environment

The voting machine operates in a certain environment in terms of its inputs and outputs. Some aspects of this environment may yield clues that it is being tested, rather than used in a normal election. For example:

- If the machine is treated in some different way when being activated for testing rather than normal voting, this is an easy thing to detect. For example, if a machine has its usual memory card replaced just before Parallel Testing, but it does not under normal circumstances, the attack program could use this to determine that it is being tested.

- Many machines require entry of authorization codes, memory tokens, or smart cards before a vote can be cast. If the same memory token/smartcard is presented many times, or if sequentially issued authorization codes are used for the voting machine, this could indicate testing.

An attacker's knowledge of these idiosyncrasies in the testing process could allow her to defeat Parallel Testing without increasing the attack team size. As long as there is something detectable by the machine that *always* occurs in Parallel Testing, the attacker should be able to defeat it. Take, for example, the situation where authorization codes are entered in tested machines sequentially. If the attacker knows that this always occurs in Parallel Testing, she simply instructs the Trojan Horse to shut off in the event that the first five authorization codes are entered sequentially. The testers would see no evidence that a Trojan Horse has been inserted into the machine.

To the furthest extent possible, the voting machine would be designed so that Parallel Testing would look no different from normal voting to the machine. More importantly, the precise techniques used for Parallel Testing (*e.g.*, exactly

how and when the machine is activated, how activation codes/smart cards/*etc.* are produced to allow voting, *etc.*) should not be fully determined or revealed until immediately before the election. For Parallel Testing to be most effective, details of how Parallel Testing is conducted would change from election to election.

Recognizing Voting Patterns

Parallel Testing means voting on the machine to verify that it is accurately collecting votes. However, some voting patterns are more likely to occur than others, and some voting patterns are almost certainly artificial. If a Trojan Horse recognizes a voting pattern as artificial, it can shut off and defeat Parallel Testing.

There are at least three ways for an attacker to exploit this vulnerability:

- The attacker could help write the Parallel Testing script, or have some power over it. She could use this to ensure that its outputs are always detected by the attack program. For example, the attacker could design the Parallel Testing script to undervote the first race on the 40th and 50th ballots cast; the attack program would notice this and refrain from any attack behavior when it happens.[139]

- The attacker could analyze the program or process used to generate the scripts (sequence of votes) used for Parallel Testing and find a way to detect these scripts. For example, if the Parallel Testing program always generates a script where the first vote is one for a Federalist, the attack program might only trigger where the first vote is for a non-Federalist candidate.

- The attacker could analyze the statistical pattern of actual ballots cast in the state or county she is attacking, and attempt to design her program to catch suspicious patterns. This involves a kind of arms race between the attacker and the designer of Parallel Testing scripts. It also involves a huge increase in the sophistication of the attack program.

An important lesson from this analysis is that to make Parallel Testing more effective, the Parallel Testing scripts need to be generated in a way that is not completely under any one person's control. The program used to generate Parallel Testing scripts would be kept secret until the day of the election; afterward, it would be fully specified, along with the random number generator seed used to produce the scripts, so that everyone can see that the scripts were generated in a sensible way and according to the program. It is important to design the Parallel Testing scripts so that they do not deviate in obvious ways from real voting patterns: that is, to be most effective, the scripts would include occasional third-party votes, undervotes, straight-ticket votes and would broadly track likely voting patterns.

If an attacker can develop a Trojan Horse that can separate real voting patterns from Parallel Testing patterns, she can subvert Parallel Testing without increasing her attack team size. On the other hand, it is important to recognize the differ-

Good Parallel Testing should make a successful Software Attack Program significantly more complex to execute successfully.

ence between a theoretical difference in voting patterns and one that is useful to an attack program. The attack program must run on voting machines in a wide variety of polling places with a wide variety of voting patterns. Refusing to activate the attack behavior for too many voting patterns would leave the attack program unable to operate, and the attacker has a daunting data analysis problem to solve before she can determine how to write her attack program.

Recognizing Usage Patterns

Finally, the attack program may recognize usage patterns from the parallel testers that differ in important ways from those of real voters. For example:

- Parallel testers are likely to vote much more quickly and efficiently than most voters, especially after having cast many previous votes.
- A team of one or two parallel testers using the machine would not vary much in their usage pattern; that is, there would not be a fast, efficient voter followed by a rather slow one as one would expect to see in a real election.
- Parallel testers are likely to have very different patterns of errors (*e.g.*, attempted overvotes, undervotes which they return to and correct) than normal voters, especially after casting many votes.
- Parallel testers may take less time between casting ballots than normal voters; in a real election, the pattern of voters coming to vote would vary during the day.
- Unless instructed to do so by the script, most parallel testers are not likely to use assistive technology or alternative languages. On the other hand, if Parallel Testing scripts always include at least one use of each alternative language, this is likely to allow the attack program to determine that it is being tested.

One lesson from this analysis is that, to be most effective, the Parallel Testing script should include details like how quickly or slowly to vote, when to make "errors," and perhaps even when to cast each vote.[140]

More generally, our review of Parallel Testing leads us to conclude that good Parallel Testing should make a successful Software Attack Program significantly more complex to execute successfully. In terms of forcing our attacker to add additional informed participants to her attack, it might only require the addition of one to three people. This could be someone in control of writing, or with access to, Parallel Testing scripts. If such persons worked in conjunction with the designer of the Trojan Horse, they would have a good chance of subverting Parallel Testing. Similarly, conspirators with excellent knowledge of Parallel Testing procedures and practices could assist in the development of a Trojan Horse that could shut off when testing was detected.

TAKING ACTION WHEN PARALLEL TESTING FINDS DISCREPANCIES

Parallel Testing provides another problem: what happens when the electronic results reported by the machine do not match the script? In California, the process is relatively straightforward: a videotape of the testing is reviewed. The testers and Parallel Testing project manager examine the tape to determine whether human error (*i.e.*, where the tester has accidentally diverged from the script) is the cause of the discrepancy.[141]

If human error cannot explain the discrepancy, the Secretary of State's office impounds the machine and attempts to determine the source of the problem. Beyond this, even California does not appear to have a clear protocol in place.[142]

We have concluded that even if Parallel Testing reveals evidence of software bugs and/or attack programs on a voting machine, this countermeasure itself will be of questionable value unless jurisdictions have in place and adhere to effective policies and procedures for investigating such evidence, and taking remedial action where appropriate. Detection of fraud without an appropriate response will not prevent attacks from succeeding. We offer an example of procedures that could allow jurisdictions to respond effectively to detection of bugs or software programs in Appendix M.

Adhering to such procedures when discrepancies are discovered during Parallel Testing is of the utmost importance. The misrecording of a single vote during Parallel Testing could indicate much wider problems.[143] Our analysis shows that Parallel Testing is a meaningful countermeasure only if there is a clear commitment to following investigative and remedial procedures when problems are discovered.

CONCLUSIONS AND OBSERVATIONS

Conclusions from the Representative Least Difficult Attack

With the Basic Set of Countermeasures in place, a minimum of one informed participant will be needed to successfully execute DRE Attack Number 4 (Trojan Horse Inserted Into Operating System) and change the result of the Pennasota governor's race.

With the Regimen for Parallel Testing Plus Basic Set of Countermeasures, DRE Attack Number 4 becomes more difficult. The attacker will need at least 2 to 4 informed participants[144] to successfully execute DRE Attack Number 4 and change the result of the Pennasota governor's race.

We are unable to examine whether the Regimen for Automatic Routine Audit Plus Basic Set of Countermeasures would make DRE Attack Number 4 more difficult because DREs do not have a voter-verified paper trail.

Conclusions about Trojan Horse and other Software Attack Programs

- The Trojan Horse and other corrupt software attacks are extremely dangerous because they require very few (if any) co-conspirators and can affect enough votes to change the outcome of a statewide race.

- The Basic Set of Countermeasures currently used in many jurisdictions is not likely to catch a clever Trojan Horse or other Software Attack Program.

Conclusions about the Potential Effectiveness of Parallel Testing

- Parallel Testing, if conducted properly, will force an attacker who employs a Software Attack Program to spend much more time preparing her attack, and gaining significant knowledge before she can execute a successful attack.

- Parallel Testing creates a kind of arms race between attackers and defenders: as Parallel Testing becomes more sophisticated, the attacker must become more sophisticated; as the attacker becomes more sophisticated, Parallel Testing must come up with new ways to trip her up. The single biggest problem with Parallel Testing is that, given the potential resources and motivation of an attacker, it is ultimately unclear whether the final advantage would lie with the testers or the attacker. Moreover, because Parallel Testing does not create an independent record of voters' choices, there is no reliable way to know whether an attack has successfully defeated Parallel Testing.

- Parallel Testing would not necessarily require an attacker to involve significantly more co-conspirators to employ her attack successfully. We have envisioned scenarios where the attacker could involve as few as one to three additional conspirators to circumvent Parallel Testing. Because of the "arms race" created by Parallel Testing, it is extremely difficult to assign a minimum number of attackers that might be needed to circumvent it.

Conclusions about Taking Action When Attacks or Bugs Are Discovered by Parallel Testing

- Parallel Testing as a countermeasure is of questionable value unless jurisdictions have in place and adhere to effective policies and procedures for investigating evidence of computer Software Attack Programs or bugs, and taking remedial action, where appropriate.

Key Observations about Parallel Testing

Our examination of Parallel Testing shows that the following techniques could make a Parallel Testing regime significantly more effective:

- The precise techniques used for Parallel Testing are not fully determined or revealed, even to the testers, until right before the election. Details of how Parallel Testing is conducted are changed from election to election.

- The wireless channels for voting machines to receive commands are closed.
- Voting machines are never connected to one another during voting. If they are normally connected, a voter or pollworker might be able to activate or deactivate a Trojan Horse on every machine in the polling place with one triggering command or event.
- Each voting machine is completely isolated during the election. This would prevent remote attacks from activating or deactivating the Trojan Horse.
- To the extent possible, the voting machines are designed so that Parallel Testing would look no different from real voting to the machine. Parallel Testing scripts could include details like how quickly or slowly to vote, when to make "errors," and perhaps even when to cast each vote.
- Parallel Testing is videotaped to ensure that a contradiction between the script and machine records when Parallel Testing is complete is not the result of tester error.

ATTACKS AGAINST DREs w/VVPT

We have identified over forty (40) potential attacks against DREs w/VVPT.[145] As it was for DREs without VVPT, all of the least difficult attacks against DREs w/VVPT involve inserting Trojan Horses or corrupt software into the DREs. The key difference in attacks against DREs w/VVP T is that our attacker may also have to attack the paper trail.

A paper trail by itself would not necessarily make an attack on DREs more difficult. An attacker against DREs w/VVPT has two options:

1. Ignore the paper trail in the attack. Under this scenario, only the electronic record of votes is targeted. The attacker hopes that the electronic record becomes the official record, and that no attempt is made to count the paper record, or to reconcile the paper and electronic records; or
2. Attack both the paper and electronic record. Under this scenario, the attacker would program her software record to change both the electronic and paper records. This attack would only work if a certain percentage of voters does not review the paper record and notice that their votes have not been recorded correctly.

In this section, we examine examples of both types of attacks. Further, we evaluate how difficult each of these attacks would become if a jurisdiction implemented the "Basic," "Parallel Testing Plus Basic," and "Automatic Routine Audit Plus Basic" sets of countermeasures.

If the vendor writes the ballot definition files for many counties in a state, only one person would be needed to trigger and parameterize the attack in many polling places.

REPRESENTATIVE "LEAST DIFFICULT" ATTACK: TROJAN HORSE TRIGGERED WITH HIDDEN COMMANDS IN BALLOT DEFINITION FILE (DRE w/VVPT ATTACK NUMBER 1A)

We have already discussed how a Trojan Horse might be inserted into a DRE. The insertion of a Software Attack Program into a DRE w/VVPT would not differ in any significant way. It could be inserted into the software or firmware at the vendor, into the operating system, COTS software, patches and updates, *etc.* In most cases, this would require the involvement of a minimum of one attacker.

As already discussed (*see supra* p. 55), if the attacker wanted to tailor her attacks to specific precincts, she might create an attack program that would not activate unless it has been triggered. In this scenario, the attack would be "parameterized" (*i.e.,* told which ballot, precinct, race, *etc.* to attack) by commands that are fed into the machine at a later time. This allows the attacker to trigger an attack with specific instructions whenever she decides it could be useful.

Voting machine security experts sometimes imagine this triggering and parameterization would happen via the ballot definition files.[146] Ballot definition files tell the machine how to (1) display the races and candidates, and (2) record the votes cast. Ballot definition files are often written by the voting machine vendor employees or consultants, but they are also frequently written by local jurisdictions themselves (at the county level), with software and assistance provided by the vendor.[147]

A seemingly innocuous entry on the ballot definition file could be used to trigger the attack program. For instance, as already discussed, an extra space after the last name of a candidate for a particular race could trigger an attack that would subtract five votes from that candidate's total on every machine. This triggering is referred to as "parameterization" because it allows the attacker to set the parameters of the attack – *i.e.,* the ballot, the precinct (because there is a different ballot definition file for each precinct), the race, and the candidate who is affected.

If the vendor writes the ballot definition files for many counties in a state, only one person would be needed to trigger and parameterize the attack in many polling places.

This attack would become more difficult if every county created its own ballot definition file. In such cases, the attacker would have to find one participant per county to help her with her attack. In addition to forcing the attacker to expand the number of participants working with her, creating the ballot definition files locally could force the attackers to infiltrate the election offices of multiple counties.

Here is how this representative attack could happen in Pennasota:[148]

- The Software Attack Program is created and inserted at any time prior to an election.

- If the ballot definition files are created at the vendor, or by a consultant provided by the vendor: Someone at the vendor involved in creating, editing or reviewing the ballot definition files would insert the commands that tell the Attack Program which race to target.

- If the ballot definition files are created by local jurisdictions: Three separate people working in the election offices of the three largest counties insert commands into the ballot definition files. Obviously, these co-conspirators would have to possess access to the ballot definition files.

- The Software Attack Program could be set to activate on a specific date and time (*e.g.*, the first Tuesday after the first Monday in November, after 11 a.m.). This would help it avoid detection during Logic and Accuracy Testing; there would be no need to worry about ITA or Acceptance Testing, as the ballot definition file is not subjected to either of these tests.

- When switching votes, the ballot definition file could show voters Tom Jefferson on the confirmation screen, but electronically record a vote for Johnny Adams.

- Alternatively, the Software Attack Program could alter votes in the electronic memory at the end of a full day of voting.

- To avoid detection after the polls have closed, the Software Attack Program could create and provide a new log to the outside world, different than the one stored internally.

In the gubernatorial election for the State of Pennasota, we have calculated that if a Trojan Horse were inserted into the ballot definition files for *only* the three largest counties, it would need to switch only four (4) votes per machine (or less than 5% of votes per machine) to change the results of our close statewide election:

- Total votes Johnny Adams needs to switch for comfortable victory: 51,891

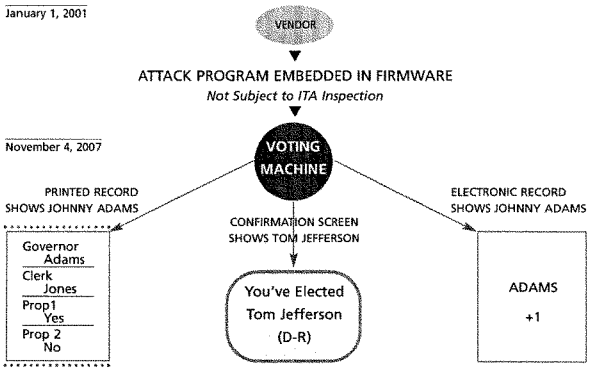
- Number of DREs w/VVPT in 3 largest counties: 9,634[149]

- If four (4) votes on each machine in the three largest counties were switched, Johnny Adams would have gained enough votes to defeat Tom Jefferson comfortably.

Thus, this attack would require between two and four participants: one to insert the Software Attack Program, plus either one or three (depending upon whether ballot definition files were created at the vendor or county) to provide triggering and parameterization commands in the ballot definition files.

FIGURE 7

POSSIBLE ATTACK ON DRE WITH VVPT



Although it might be more difficult than other types of Trojan Horse attacks (because it could require one informed participant per county, as opposed to a single informed participant via several points of entry), the "Trojan Horse Triggered by Hidden Commands in the Ballot Definition File" attack has certain elements that would render it less difficult to execute:

- This attack provides the attackers a great deal of flexibility. The attackers can wait until just before any election to trigger an attack, and their attack can target specific precincts.

- This attack is reusable. The attack program would not do anything unless it receives commands from ballot definition files. These commands could come before any election and the attack program could lie dormant and undetected for many election cycles.

ATTACKING BOTH PAPER AND ELECTRONIC RECORDS (DRE w/VVPT ATTACK NUMBER 6)

In the above analysis, we assumed that the paper trail is not attacked: only the electronic record misrecorded the vote. Would not this mean that the attack would be detected? Not necessarily.

Even in states with mandatory voter-verified paper trails, official vote totals are still extracted from the electronic record of the machine. While an attacker might have to worry that a VVPT recount in a close race would expose the attack, statewide recounts are still relatively rare.[150]

PAPER MISRECORDS VOTE

To prevent an attack from being noticed in a recount, our attacker could create a Software Attack Program that also directs the printer to record the wrong vote. This "Paper Misrecords Vote" attack is Attack Number 6 in the DRE w/VVPT Catalog.

The attack could work the same way as DRE w/VVPT Attack Number 1a (Trojan Horse Triggered with Hidden Commands in Ballot Definition File),[151] except that it would add a step: the paper receipt printed after the voter has made all of her selections would incorrectly record her vote for governor. In practice, this is how it would work:

- When a targeted voter chooses Tom Jefferson, the screen would indicate that she has voted for Tom Jefferson.
- After she has completed voting in all other races, the DRE would print a paper record that lists her choices for every race, except for governor. Under the governor's race, it would state that she has selected Johnny Adams.
- When the DRE screen asks the voter to confirm that the paper has recorded her vote correctly, one of two things would happen:
  - The voter would fail to notice that the paper has misrecorded the vote and accept the paper recording; or
  - The voter would reject the paper record, and opt to vote again.
- If the voter rejects the paper record, the second time around it would show that she voted for Tom Jefferson. This might lead her to believe she had accidentally pressed the wrong candidate the first time. In any event, it might make her less likely to tell anyone that the machine made a mistake.

This attack would not require any additional participants in the conspiracy. Nor

is it entirely clear that enough voters would notice the misrecorded votes to prevent the attack from working.

DO VOTERS REVIEW VVPT?

In a recent study, Professor Ted Selker and Sharon Cohen of MIT paid 36 subjects to vote on DRE w/VVPT machines.[152] They reported that "[o]ut of 108 elections that contained errors . . . only 3 [errors were recognized] while using the VVPT system."[153]

If only 3 of every 108 voters noticed when the paper trail misrecorded a vote for Tom Jefferson as a vote for Johnny Adams, DRE w/VVPT Attack Number 6 would probably work. If the Trojan Horse targeted approximately 54,000 voters for Tom Jefferson (or roughly 1 in every 9 voters for Tom Jefferson in the three largest counties), the vast majority would not notice that the paper had misrecorded their votes. 3% – or 1,633 – would notice. These voters would cancel the paper record and vote again. The second time, the paper would record their votes correctly.

FIGURE 8

WHERE 3 % OF VOTERS CHECK VVPT

51,891	Total votes Johnny Adams needs to switch for comfortable victory
3,459,379	Total votes
54,437	Votes attacked
3.0%	% of voters who study VVPT carefully
1,633	number of rejections of misrecorded votes
52,804	number of votes successfully switched

This would still leave enough switched votes for Johnny Adams to win the governor's race comfortably. We do not know how many of the 1,633 voters who rejected their votes would complain to poll workers that the machines had initially misrecorded their votes. But even if 50% of those voters were to complain,[154] this would be an exceptionally small number of complaints. With nearly 1,700 precincts and 10,000 DREs w/VVPT in the three largest counties, 820 complaints amount to less than one complaint per two precincts and twelve machines.[155]

We are skeptical that in the State of Pennasota, only 3% of voters would notice if their choice for governor was misrecorded on the paper trail. This is because (1) the race that we are looking at is for the top office in the state; this is an election with which voters are more likely to be concerned and, consequently, they would be more likely to check that the VVPT has correctly recorded their votes

(as opposed to their votes for, say Proposition 42, which is likely to be in the middle or bottom of their paper trail), and (2) in an actual election (as opposed to the MIT study), where candidates should be well known to most voters, they are probably more likely to notice if the paper trail accurately reflects their choice.

Convincing voters to review their VVPT is critical to its effectiveness as a measure to thwart certain Trojan Horse attacks.

Keeping in mind that the attacker's goal is to switch 51,891 votes, let us assume that 20% of all voters for Tom Jefferson in our three targeted counties would check to see that the paper has accurately recorded their votes. The attacker could reach her goal by targeting 66,000 voters for Tom Jefferson (out of nearly 1.1 million votes cast in these counties). Over 13,200 of these voters would notice that the paper misrecorded their choice; they would recast their votes. But over 52,800 would not notice; these extra 52,800 votes would be sufficient to change the outcome of the election.

FIGURE 9

WHERE 20% OF VOTERS CHECK VVPT

51,891	Total votes Johnny Adams needs to switch for comfortable victory
3,459,379	Total votes
66,004	Votes attacked
20.0%	% of voters who study VVPT carefully
13,201	number of rejections of misrecorded votes
52,804	number of votes successfully switched

It might be argued that if 13,200 people noticed that their votes had been misrecorded on the VVPT, someone would realize that something was wrong with the machines. The truth is, we cannot know what would happen if this number of people were to notice that their votes were misrecorded. As already discussed, many people would probably presume that the mistake was theirs and not that of the machine.

By contrast, if 80% of voters for Tom Jefferson in the three counties checked their paper records thoroughly, it is doubtful the attack could succeed. The Trojan Horse would have to target over 264,000 voters for Tom Jefferson to get the 51,891 needed to ensure victory for Johnny Adams. 211,212 voters for Tom Jefferson would notice that the paper trail initially recorded their votes incorrectly; this represents over 40% of all of his votes in the three largest counties.

We can see from this analysis that convincing voters to review their VVPT is critical to its effectiveness as a measure to thwart certain Trojan Horse attacks.

The Trojan Horse could be programmed in a way that would allow it to detect whether it is being tested.

THE EFFECT OF REGIMEN FOR PARALLEL TESTING PLUS BASIC SET OF COUNTERMEASURES

Our analysis of the effect of the Basic Set and Regimen for Parallel Testing Plus Basic Set of Countermeasures against the least difficult attack for DREs w/VVPT does not dramatically change from the same analysis done for DREs without VVPT. Unless voters check the paper trail and report suspected misrecordings to poll workers when they occur, the paper trail, by itself, provides very little additional security.

The Regimen for Parallel Testing Plus Basic Set of Countermeasures should provide more protection than just the Basic Set of Countermeasures. In fact, if the Software Attack Program does not recognize that it is being tested, Parallel Testing would probably catch this type of attack; presumably at least one tester would notice that the paper record was not recording correctly.

However, as already discussed, *supra* pp. 55-59, we have concerns about certain vulnerabilities in Parallel Testing: first, there is the possibility that the person installing the ballot definition file commands triggering the attack program would know which precincts are going to be subject to Parallel Testing – in California, precincts are told at least one month in advance whether their machines will be tested.[136] If the attacker knows where the Parallel Testing is going to occur, she can simply refrain from inserting the triggering commands in ballot definition files for those precincts.

Second, the attacker could, via a wireless communication or Cryptic Knock (1) activate the Trojan Horse on machines she sees are not being tested on Election Day, or (2) de-activate the Trojan Horse on machines she sees are being tested on Election Day (this presumes that Parallel Testing is done at the polling stations).

Finally, the Trojan Horse could have been programmed in a way that would allow it to detect whether it is being tested: if the attacker knew something about the testing script in advance or had a good understanding of Parallel Testing procedures, she might be able to program the Trojan Horse to shut off during all Parallel Testing.

As already discussed, the successful subversion of Parallel Testing, while adding significant complexity to a software attack, might require the additional participation of between only one and three extra informed participants.

EFFECT OF REGIMEN FOR AUTOMATIC ROUTINE AUDIT PLUS BASIC SET OF COUNTERMEASURES

The Regimen for Automatic Routine Audit Plus Basic Set of Countermeasures, if instituted as detailed *supra* pp. 16–18, should be an effective countermeasure against our least difficult attack. As detailed in Appendix K, if 2% of all

machines were audited, auditors should have a greater than 95% chance of discovering a mismatch between electronic records and paper records, where a Trojan Horse misrecorded a voter's choice in the paper record. This, of course, presumes that the attacker failed to find a way to subvert the Regimen for Automatic Routine Audit.

We have identified at least four ways an attacker could subvert the Regimen for Automatic Routine Audit:

1. The Trojan Horse attacks both paper and electronic records, and most voters do not review the paper record before casting their votes, resulting in an attack that successfully subverts both the electronic and paper record.

2. The selection of auditors is co-opted.

3. The paper record is replaced before an audit of the voter-verified paper record takes place, for the purpose of matching paper records to corrupted electronic records.

4. The paper record is replaced merely to add votes for one candidate, without regard to what has occurred in electronic record.

As with our analysis of the Regimen for Parallel Testing, to determine the likely effectiveness of the Regimen for Automatic Routine Audit, we must ask how much more difficult it would make our least difficult attack. This means, among other things, examining how many people it would take to subvert the Regimen for Automatic Routine Audit by each of the four methods listed above.

TROJAN HORSE ATTACKS PAPER AT TIME OF VOTING, VOTERS FAIL TO REVIEW

Our attacker does not necessarily need to attack the audit process directly to subvert it. What if, as already described in our discussion of DRE w/VVPT Attack Number 6 (*see supra* p. 65–67), the attacker merely designs a Trojan Horse that changes both the paper and electronic record?

As noted above, if 80% of voters thoroughly reviewed their paper trails, it is very likely that an attack on the paper trail at the time of voting would fail. Assuming, however, that this attack is noticed by voters for Tom Jefferson only 20% of the time, how much more difficult would the Regimen for Automatic Routine Audit make the attack?

If the audit of the voter-verified paper record merely adds up total votes on paper and compares them to total votes in the electronic record, it is doubtful this attack would be discovered by election officials. The paper record would match the electronic record. The attacker would not need to add any people to her conspiracy to succeed.

Jurisdictions will have to put in place certain rules regarding what is to be done when anomalies are found.

If, on the other hand, the audit of the voter-verified paper record looks for statistical anomalies by, for instance, looking at the number of times voters cancelled the paper record of their vote, this attack is likely to be caught. As already noted in Figure 9, if 20% of targeted voters notice that their paper record has not correctly recorded their vote for Tom Jefferson, there would be more than 13,000 cancellations showing Johnny Adams' name crossed out, and subsequently replaced by Tom Jefferson:

51,891	Total votes Johnny Adams needs to switch for comfortable victory
3,459,379	Total votes
66,004	Votes attacked
20.0%	% of voters who study VVPT carefully
13,201	Number of rejections of misrecorded votes
52,803	Number of votes successfully switched

While 13,201 votes is an extremely small percentage of the 3.4 million votes cast, it would represent an unusually large number of cancellations. Larry Lomax, Registrar of Voters for Clark County, Nevada (which has used DREs w/VVPT since 2004) states that in Clark County it is "the exception" to find a single cancellation on a DRE's entire roll of paper trail.[157] Even if we were to assume that it is normal to have one cancellation for every two DREs w/VVPT, this would mean that in Pennasota, there would ordinarily be about 14,000-15,000 cancellations in the entire state.[158] Thus, an audit of the voter-verified paper record that looked for statistical anomalies like cancellations would show that there were 90% more cancellations than normal.

An audit of the voter-verified paper record that noted which votes were changed after cancellation would show an even more troubling pattern: a highly disproportionate number of cancellations where the paper record changed from Johnny Adams to Tom Jefferson.

Finally, to the extent this attack is limited to the smallest possible number of polling places in three counties (as we originally suggested), certain audits would show an even higher statistical anomaly – with an additional 22 paper cancellations per polling place.[159]

Of course, finding statistical anomalies, no matter how troubling, would not, *in and of itself,* thwart an attack. Jurisdictions will have to put in place certain rules regarding what is to be done when such anomalies are found.

Other than requiring auditors and election officials to look for discrepancies between paper and electronic records, states do not currently mandate review of paper records for statistical anomalies. States that do not review statistical anomalies (such as, for instance, an unusually high number of cancellations or skipped races) during audit will remain vulnerable to a number of attacks.

Our analysis shows that unless a jurisdiction implements and adheres to effective policies and procedures for investigating such anomalies (and taking remedial action, where appropriate), a review of statistical anomalies will be of questionable security value. We provide examples of procedures that would allow jurisdictions to respond effectively to detection of statistical anomalies in the voter-verified paper record in Appendix M.

CO-OPTING THE AUDITORS

An obvious, but difficult way to subvert the audit is to directly co-opt the auditors. However, given the fact that under the Regimen for Automatic Routine Audit audit teams are randomly assigned to randomly selected voting machines, it would be exceptionally difficult to defeat the Regimen for Automatic Routine Audit by co-opting the auditors. We have estimated that in an audit of 2% of all machines, there would be 386 auditors randomly assigned to machines in the three largest counties in Pennasota.[160] As demonstrated in Appendix L, to have a reasonable chance of subverting the audit by infiltrating the auditors, it would be necessary to subvert all of them.

Of course, if a corrupt person selects the auditors or polling places and does not follow the "transparent random selection process" discussed *supra* p. 17, subversion of the Automatic Routine Audit becomes much easier. For instance, if the attacker were in control of the decision as to which polling places to pick for the audit, she could deliberately choose those polling places that she knows the Trojan Horse did not attack. For this reason, transparent randomness (as discussed in detail in Appendix F) is critical to an effective audit.

REPLACING PAPER BEFORE THE AUTOMATIC ROUTINE AUDIT TAKES PLACE

Another way to subvert the Regimen for Automatic Routine Audit is to replace the paper before an audit can be completed, for the purpose of making sure that the audited paper records match the corrupted electronic records. This would be nearly impossible if the audit of the voter-verified paper record was conducted in the polling places immediately after the polls close.

We understand that for many jurisdictions, this will not be realistic. After spending all day at the polls, it is likely that pollworkers and election officials would not want to spend additional time assisting auditors as they conduct an audit of the voter-verified paper record. Moreover, many audit volunteers may be reluctant to begin conducting an audit (which would, at the very least, take several hours) at 9 or 10 p.m.

If the audit of the voter-verified paper record is not conducted at the polls immediately upon their closing, there are at least two ways in which an attacker could corrupt or replace the paper trail: (1) by intercepting and replacing the paper while it is in transit to the warehouse or county offices where the audit would take place, or (2) by replacing the paper where it is stored prior to the audit.

If there are very strong physical security measures, such as those assumed in the Basic Set of Countermeasures, and paper from each polling place is delivered to the audit location separately, task (1) would be extremely difficult. Even assuming the attackers have attacked the minimum number of polling places (606), they would need to intercept and replace more than 550 separate convoys of paper to have even a one in three chance that the audit would not catch the fact that some paper record had different totals than the electronic record.[161] Given that in most states all polls close at the same time, this would seem to require the participation of at least 1,100 additional informed participants, making the attack far more difficult.

The alternative would be to attempt to replace the paper records at the county warehouses, prior to the audit. As already discussed, our assumption is that our attackers would need to target a minimum of three counties to change the outcome of the governor's race in Pennasota. This means, at a minimum, that our attackers would need to target three separate county warehouses and replace the paper records stored there.

Again, if very strong physical security measures and the chain of custody practices assumed in the Basic Set of Countermeasures are followed, this should be very difficult.

We have estimated that 2,883 DREs w/VVPT would have to be replaced to change the outcome of a statewide race.[162] In Pennasaota, the voter-verified paper records of each of these machines would have been sealed with tamper evident seals and stored in a room with perimeter alarms, secure locks, video surveillance, and there would be regular visits by security guards and police officers. The seal numbers would have been assigned at the polling place and logged by county officials upon reaching the county warehouse.

We have assumed that the audit of the voter-verified paper record would begin at 9 a.m. the morning after the polls closed, so our attackers would have to subvert all of these precautions and replace the paper trails for nearly 2,117 DREs w/VVPT in three county warehouses within a matter of hours to ensure that the attack was not discovered during the audit.[163]

Aside from the fact that, in Pennasota, our attackers would (in this very short time period) need to (1) break and replace thousands of tamper-evident seals in three separate locations,[164] (2) get past the warehouse locks and alarms, (3) co-opt (or avoid detection by) the randomly assigned police officers and security guards at each location,[165] and (4) somehow avoid detection by the video surveillance, the attackers would also need to deliver and replace 2,117 rolls of VVPT (or, in the case of PCOS, about 40,000 separate ballots) without independent observers outside or inside the warehouse noticing. We have concluded that it would not be feasible to carry out this attack without detection over such a short period of time, unless the attackers had the cooperation of hundreds of participants including many insiders (*i.e.*, security guards, policemen and video-monitors).

REPLACING SOME PAPER RECORDS MERELY TO ADD VOTES

Our attackers have a final option: attack the paper records, not for the purpose of reconciling them with the electronic records, but merely to add enough paper votes to Adams's total to ensure that the paper records also show him winning. This would merely mean stuffing enough ballot boxes with additional ballots to give Adams a majority of votes in the paper record.

The audit of the voter-verified paper record would then show a discrepancy between the electronic and paper records. A recount would follow. It would show that Adams had more votes in the paper record. In 15 states, the VVPT laws specify that "if there is a recount, the paper ballot" is the official record.[166]

There are a number of problems associated with a bright line rule stating that the paper (or electronic) record will always control election results. There is certainly nothing wrong with providing that paper records will have a "presumption" of authority. A bright line rule, however, could invite the kind of deception we are seeking to prevent.

As this analysis shows, the main benefit of paper, when accompanied by the Regimen for Automatic Routine Audit, is that it requires the attackers to subvert *both* the electronic and paper records. If the attackers know that they only have to attack the paper record, their attack becomes significantly easier.

In our scenario, the attackers would successfully insert the Trojan Horse. Obviously, they would not have to do this if they knew the paper record always controlled. They could merely attack the paper record and hope the audit of the voter-verified paper record would spot a contradiction between the paper and electronic records (which it almost certainly would if they switched enough votes to change the outcome of the election).

But let us suppose they did insert the Trojan Horse. If they intercepted 60 convoys of paper (or merely replaced several ballot boxes in 60 polling places before they were transported), they could replace enough paper to create a victory for Johnny Adams in the paper record as well.[167] While not easy, this attack is clearly much easier (involving at least 1,000 fewer participants) than one that would require the attackers to prevent the audit of the voter-verified paper record from revealing contradictory paper and electronic records.

Of course, when the audit of the voter-verified paper record was conducted, Pennasota would discover that something strange had happened: in at least a few audited polling places, the paper and electronic records would not match.

But this would not tell Pennasota who won. A recount would show Johnny Adams winning under either set of records. A bright line rule about which record should govern in such circumstances is problematic. It would encourage the kind of deception we have imagined in this attack: if Pennasota had a law stating paper

records should govern (as provided in California),[168] Johnny Adams would win. If the law stated that electronic records govern (as provided in Idaho and Nevada),[169] Johnny Adams would still win.

What can be done to prevent this attack? We discuss this below.

TAKING ACTION WHEN AUTOMATIC ROUTINE AUDIT FINDS ANOMALIES

Many state statutes are silent as to what should happen when paper and electronic records cannot be reconciled. As already discussed, Illinois law provides that where electronic and paper records in the Automatic Routine Audit do not match, the county notifies "the State Board of Elections, the State's Attorney and other appropriate law enforcement agencies, the county leader of each political party, and qualified civic organizations."[170]

As with Parallel Testing, an Automatic Routine Audit offers questionable security benefit unless effective procedures to investigate discrepancies (including taking remedial action, where necessary) are implemented and adhered to. Again, detection of possible fraud without an effective response will not thwart an attack on voting systems. The following are examples of procedures that would allow jurisdictions to respond effectively to discrepancies between paper and electronic records during an Automatic Routine Audit:

1. Conduct a transparent investigation on all machines where the paper and electronic records do not match to determine whether there is any evidence that tampering with the paper records has occurred.[171]

2. To the extent that there is no record that the paper records have been tampered with, certify the paper records.

3. If there is evidence that the paper records have been tampered with, give a presumption of authority to the electronic records.

4. After giving a presumption of authority to the electronic records, conduct a forensic investigation on all machines where the paper and electronic records do not match. The purpose of this investigation would be to determine whether there has been any tampering with the electronic records.

5. If tampering with the electronic records can be ruled out, certify the electronic records.[172]

6. Where there is evidence that both sets of records have been tampered with, conduct a full recount to determine whether and to what extent paper and electronic records cannot be reconciled.

7. At the conclusion of the full recount, determine the total number of machines that report different electronic and paper records.

8. After quantifying the number of machines that have been tampered with, determine the margin of victory in each potentially affected race.

9. Based upon (a) the margin of victory, (b) the number of machines affected, and (c) the nature and scope of the tampering, determine whether there is a substantial likelihood that tampering changed the outcome of a particular race.

10. In the event that a determination is made that there is a substantial likelihood that tampering changed the outcome of a particular race, hold a new election for the office.

CONCLUSIONS

Conclusions from the Representative Least Difficult Attack

- Assuming that only 20% of voters review their voter-verified paper trail, a minimum of one to three informed participants[173] will be needed to successfully execute DRE w/VVPT Attack Number 6 (Memory and Paper Misrecord Vote Due to Trojan Horse Inserted in Ballot Definition File) and change the result of the Pennasota governor's race.

- Assuming that 80% of voters review their voter-verified paper trail, DRE w/VVPT Attack Number 6 will not succeed.

- With the Parallel Testing Regimen Plus Basic Set of Countermeasures, DRE w/VVPT Attack Number 6 becomes more difficult. The attacker will need at least 2 to 6 informed participants to successfully execute DRE w/VVPT Attack Number 6 and change the result of the Pennasota governor's race.

- DRE Attack w/VVPT Attack Number 6 would be substantially more difficult to successfully execute against the Basic Set of Countermeasures Plus the Automatic Routine Audit Regimen than it would be against the Basic Set of Countermeasures or the Parallel Testing Regimen Plus Basic Set of Countermeasures. The attacker will need at least 386 informed participants to successfully execute DRE w/VVPT Attack Number 6 and change the result of the Pennasota governor's race.

Conclusions about the DRE w/VVPT

- As with DREs without VVPT, local jurisdictions that take control of important tasks, like creating ballot definition files, will make successful statewide attacks more difficult.
- The value of paper without an Automatic Routine Audit against many attacks (such as DRE Attack Number 1a, where the electronic record is changed, but the paper record is not) is highly questionable.
- If voters are encouraged to review their VVPT thoroughly before casting their votes, many of the least difficult attacks against DREs w/VVPT will become substantially more difficult.

Conclusions about the Regimen for Automatic Routine Audit Plus Basic Set of Countermeasures

- Statistical examination of anomalies, such as higher than expected cancellations, can help to detect fraud. Currently, none of the states that conduct routine audits of voter-verified paper records examine those paper records for statistical anomalies.
- Automatic Routine Audits conducted soon after the close of polls are less vulnerable to attack because there is less time to tamper with the paper records.
- Good chain of custody practices and physical security of paper records prior to the Automatic Routine Audit is crucial to creating an effective auditing regimen. Specifically, the following practices should make the auditing process more secure:
  - At close of the polls, vote tallies for each machine are totaled and compared with number of persons that have signed the poll books.
  - A copy of totals for each machine is posted at each polling place on election night.
  - All audit information (*i.e.,* Event Logs, VVPT records, paper ballots, machine printouts of totals) that is not electronically transmitted as part of the unofficial upload to the central election office, is delivered in official, sealed and hand-delivered information packets or boxes. All seals are tamper-resistant.
  - Transportation of information packets is completed by at least two election officials representing opposing parties who have been instructed to remain in joint custody of the information packets or boxes from the moment they leave the precinct to the moment they arrive at the county election center.

- Each polling place sends its information packets or boxes to the county election center separately, rather than having one truck or person pick up this data from multiple polling locations.

- Once the sealed information packets or boxes have reached the county election center, they are logged. Numbers on the seals are checked to ensure that they have not been replaced. Any broken or replaced seals are logged. Intact seals are left intact by officials.

- After the packets and/or boxes have been logged, they are provided with physical security precautions at least as great as those listed for voting machines, above. Specifically: the room in which they are stored would have perimeter alarms, secure locks, video surveillance and regular visits by security guards and access to the room would be controlled by sign-in, possibly with card keys or similar automatic logging of entry and exit for regular staff.

- The auditing process will be much less vulnerable to attack if machines and auditors are selected and assigned in a publicly transparent and random manner.

An automatic routine audit offers questionable security benefit unless effective procedures to investigate discrepancies (including taking remedial action, where necessary) are consistently implemented.

Conclusions about Taking Action When Anomalies Are Found in the Automatic Routine Audit

An automatic routine audit offers questionable security benefit unless effective procedures to investigate discrepancies (including taking remedial action, where necessary) are consistently implemented. Detection of possible fraud without an effective response will not thwart an attack on voting systems.

ATTACKS AGAINST PCOS

We have identified over forty (40) potential attacks against PCOS. Many of these attacks are similar to the attacks against both DRE systems.

Nothing in our research or analysis has shown that a Trojan Horse or other Software Attack Program would be more difficult against PCOS systems than they are against DREs. All of the least difficult attacks against PCOS involve the insertion of Trojan Horses or corrupt software into PCOS scanners.[174] In this section, we examine how this attack would work, and how much more "expensive" such attacks would be made by the "Basic," "Regimen for Parallel Testing Plus Basic" and "Regimen for Automatic Routine Audit Plus Basic" sets of countermeasures.

We also address certain security concerns that are unique to the PCOS system.

REPRESENTATIVE "LEAST DIFFICULT" ATTACK: SOFTWARE ATTACK INSERTED ON MEMORY CARDS (PCOS ATTACK NUMBER 41)

We have already discussed how a Trojan Horse might be inserted into both types of DRE systems. The insertion of a Trojan Horse into a PCOS scanner would not differ in any significant way. It could be inserted into the main PCOS source code tree, operating system, COTS software, and software patches and updates, *etc. In most cases, this would require the involvement of a minimum of one person.*

Attack Number 41 in the PCOS Catalog is an attack that has been demonstrated to work in at least two election simulations:[175] use of memory cards to change the electronic results reported by the PCOS scanner. While this attack has only been publicly attempted against one model of PCOS scanner, several computer security experts who have reviewed other PCOS systems believe that they may be vulnerable to similar attacks.[176]

DESCRIPTION OF ATTACK

This attack uses replaceable memory cards to install the software attack. Memory cards are used by both DREs and PCOS scanners. Memory cards contain data that is used by the machines, including the ballot definition files (which allow the machine to read the ballots) and the vote totals. At least one major vendor has its report generation program on its memory cards – this is the program that, among other things, tells the machine what vote totals to print at the close of the polls. This is the record pollworkers use to record the final vote tally of each machine.

Attackers could use the memory cards to generate false vote total reports from the machine. Here is how the attack would work:

- The attacker acquires access to the memory cards before they are sent to individual polling places. She could gain access:
  - At the county office where they are programmed, if she works there, or if security is lax.
  - Via modem, if the central tabulator[177] that programs the cards is connected to a telephone line.
  - Via modem if the PCOS that reads the cards is connected to a telephone line.
- The attacker programs the memory cards to generate a vote total that switches several votes from the Democratic-Republicans to the Federalists (or from Jefferson to Adams).

- She further instructs the memory card to generate the false total only if 400 ballots have run through the scanner in a single 24-hour period (unlike DREs, PCOS scanners can scan hundreds or thousands of votes in a single day). This should help it avoid detection during Logic and Accuracy Testing.

- The attacker does not have to worry about ITA inspection or testing or Acceptance testing because the memory cards are not subject to ITA inspection or testing and are created after Acceptance Testing is complete.

- At the close of the polls, when election officials and/or poll workers ask the PCOS scanner to generate its vote total report, the false report would be generated.

As with Trojan Horse Attacks and other Software Attack Programs used against DREs, the attackers could target a relatively small number of machines and still change the outcome of our statewide race.

We have assumed that the State of Pennasota has purchased one PCOS machine for each precinct.[178] This would mean that in its three largest counties, there would be a total of 1,669 PCOS machines, with approximately 693 voters per machine. In the entire state, there would be 4,820 machines, with approximately 718 voters per machines.[179]

Again, presuming that our attacker wants to switch 51,891 votes from Tom Jefferson to Johnny Adams, she could target fewer than half of the machines in the three largest counties, switching about 7% of the votes for governor on each machine.[180] On the other hand, if the attacker chose to target all PCOS scanners in the state, it would be necessary to switch only about 8 votes per machine (or slightly more than 1% of all votes cast on each machine).[181]

As with the Software Attacks against DREs previously discussed, if the Software Attack Program functioned as intended (and presuming there was no recount, Parallel Testing or audit), there would be no way for election officials to know that the electronic records were tampered with.

This attack would require a minimum of one to three people: one if the central tabulators in several counties are connected to a telephone line (in which case, an attack could hack into the central tabulators and insert the attack program into the memory cards via the central tabulator), and three if the state made sure that there was no way to contact the central tabulators or PCOS machines via modem or wireless communication (in which case, three individuals would have to gain access to the county offices in the three largest counties and program or reprogram the memory cards before they were sent to the polling places).

EFFECT OF BASIC SET OF COUNTERMEASURES

Our analysis of the three sets of countermeasures is substantially similar to our analysis in the DRE w/VVPT section.

This attack is not likely to be caught by the Basic Set of Countermeasures. Memory cards are not subject to ITA or Acceptance Testing. If the attacker is clever, she should be able to ensure that Logic and Accuracy Testing does not catch this attack either. The memory cards are inserted in the normal course of election practice; physical security around the machines and ballots would not prevent successful execution of the attack.

EFFECT OF REGIMEN FOR PARALLEL TESTING PLUS BASIC SET OF COUNTERMEASURES

We are unaware of any jurisdiction that performs Parallel Testing on PCOS systems. Nevertheless, we believe that Parallel Testing would probably catch this attack. Unlike Trojan Horses and other Software Attack Programs previously discussed, the attack would probably not allow the PCOS to know whether it was being Parallel Tested.[182]

However, our concerns regarding the ability of other types of Software Attack Programs to circumvent Parallel Testing (*i.e.,* the insertion of a Trojan Horse into firmware, vendor software, COTS software, software patches and updates) apply to PCOS for the same reasons already detailed in our discussion of attacks against DREs. Specifically, we believe that under the right circumstances and with enough knowledge and time, it would be possible to devise a Software Attack Program against PCOS systems that would allow the scanners to trigger or deactivate based upon the program's ability to detect whether the scanner is being tested.

Thus, if the attacker knew that Parallel Testing was performed on PCOS machines in Pennasota, she could insert a Trojan Horse that would recognize if the machine was being Parallel Tested. *This would require involving between one and three additional people in the attack:* specifically the attack would need to involve people who could gain enough knowledge about the Parallel Testing regime (*i.e.,* the Parallel Testing script writer, a consultant who worked on creating the Parallel Testing procedures) to provide information to subvert it.

EFFECT OF REGIMEN FOR AUTOMATIC ROUTINE AUDIT PLUS BASIC SET OF COUNTERMEASURES

All of our findings regarding the Regimen for Automatic Routine Audit in the DRE w/VVPT section apply to the Automatic Routine Audit as a countermeasure against the least difficult attack against PCOS. If the Regimen for Automatic Routine Audit is fully implemented (including the use of transparent randomness in selecting auditors and polling places for audit, as well as instituting proper chain of custody and paper security practices), *the Regimen for Automatic Routine Audit Plus Basic Set of Countermeasures should make the least difficult attack against PCOS more difficult by several hundred participants.*

However, at least two of the attacks in our attack catalog point us to unique issues associated with PCOS and the Regimen for Automatic Routine Audit countermeasures.

PCOS Attack Number 42:
Trojan Horse Disables Overvote Protections

One of the benefits of PCOS machines over Central Count Optical Scanners (which are very often used in tallying absentee ballots) is that it has an "over/undervote protection." The attack discussed below is a variant of the Trojan Horse attacks already discussed[183] with one important exception: instead of changing votes or the vote total tally, it merely disables the over/undervote protection.

The over/undervote protection on PCOS scanners works as follows: when a voter fills out his ballot, but accidentally skips a race (or accidentally fills in two candidates for the same race), the scanner would refuse to record the vote and send it back to the voter for examination. The voter than has the opportunity to review the ballot and correct it before resubmitting.

Central Count Optical Scanners have been shown to lose as many as three times as many votes as PCOS.[184] The lack of over/undervote protection on Central Count Optical Scanners may be the reason for this difference. In counties with over 30% African American voters, the lost or "residual" vote rate has been shown to be as high as 4.1%.[185]

Our attacker in Pennasota would probably not be able to swing the gubernatorial race from Jefferson to Adams merely by inserting a Software Attack Program that would turn off the over/undervote protection on PCOS scanners. Even if we assume that the result of turning off the protection were a loss of 4% of the votes on every scanner and that all of those votes would have gone to Tom Jefferson, this would only result in the loss of about 20,000 votes. This would still leave Jefferson (who won by over 80,000) with a comfortable (though slimmer) margin of victory.

Nevertheless, this attack could cause the loss of thousands of votes, disproportionately affecting poor and minority voters. Neither the Basic Set nor Automatic Routine Audit Plus Basic Set of Countermeasures (without some sort of statistical analysis of over/undervotes) would counter this attack.

There are at least two possible ways to catch this attack:

- Through Parallel Testing (assuming that the Software Attack Program has not also figured out a way to shut off when it is being tested); and
- By counting over/undervotes in the audit of the voter-verified paper record to determine whether there is a disproportionate number of such lost votes *(this again points to the importance of statistical analysis and investigation in conjunction with the audit of the voter-verified paper record – by looking for an unusual number of over- and undervotes, the state could spot this kind of attack).*

PCOS Attack Number 49: Attack on Scanner Configuration Causes Misrecording of Votes

Advocates for PCOS systems point out that the paper record is created by the voter, rather than a machine; the purported benefit of voter-created paper records is that they cannot be corrupted by the machine (as in DRE w/VVPT Attack Number 6, where the machine creates an incorrect paper record).

The flip side of this benefit is that, in filling out their ballots, people can make mistakes: they might circle the oval instead of filling it in; they might fill in only half the oval; they might fill the oval in with a pencil that the machine cannot recognize. If our attackers configured our machines so that they tended to read partially filled ovals for Johnny Adams, but not Tom Jefferson, Johnny Adams could benefit with many additional votes. Given our analysis of PCOS Attack Number 8, we are skeptical that this attack would be sufficient to turn our imagined election from Jefferson to Adams (though without more investigation, we are unable to come to a certain conclusion). Nevertheless, we are confident that if PCOS Attack Number 49 were accomplished via an Attack Program that reached every PCOS scanner, it probably could affect thousands of votes.

This attack highlights a problem that is unique to the PCOS system. In conducting an audit of the voter-verified paper record or recount, what should be counted as a vote? If the test is merely what the machine reads as a vote, Attack Number 49 would succeed without further investigation.

Again, some statistical analysis done in conjunction with the Automatic Routine Audit (perhaps allowing the Secretary of State's office to review ballot images to look for discrepancies in how votes are counted by the scanners) should allow a jurisdiction to catch this attack.

CONCLUSIONS

Conclusions from Representative Least Difficult Attacks

With the Basic Set of Countermeasures in place, a minimum of 1 to 3 informed participants would be needed to successfully execute PCOS Attack Number 41 (Software Attack on Inserted Memory Cards) and change the result of the Pennasota governor's race.

With the Regimen for Parallel Testing Plus Basic Set of Countermeasures in place, PCOS Attack Number 41 becomes more difficult. The attacker will need at least 3 to 7 informed participants to successfully execute this attack and change the result of the Pennasota governor's race.

PCOS Attack Number 41 would be substantially more difficult to successfully execute against the Regimen for Automatic Routine Audit Plus Basic Set of Countermeasures than it would be against the Basic Set of Countermeasures or the Regimen for Parallel Testing Plus Basic Set of Countermeasures. The attacker will need at least 386 informed participants to successfully execute PCOS Attack Number 41 and change the result of the Pennasota governor's race.

Conclusions about PCOS

- As with DREs, local jurisdictions that take more control of running their own elections (by performing their own programming, creating their own ballot definition files, *etc.*), are going to make successful attacks against statewide elections more difficult.
- The value of paper ballots without the Automatic Routine Audits is highly questionable.
- If voters are well informed as to how to properly fill out PCOS ballots, many attacks against PCOS systems will become more difficult.

Conclusions about the Regimen for Automatic Routine Audit Countermeasure

- Statistical examination of anomalies in ballot images and vote totals, such as higher than expected over- and undervotes, can help detect fraud. Currently, none of the states that conduct Automatic Routine Audits examine paper records for statistical anomalies.
- Automatic Routine Audits conducted soon after the close of polls are less vulnerable to attack, because there is less time to tamper with the paper records.
- Solid chain of custody practices and physical security of paper records prior

to the Automatic Routine Audit are crucial to creating an effective auditing regimen. The practices discussed *infra* pp. 87–88 should assist jurisdictions in creating an effective auditing regimen.

- The auditing process will be much less vulnerable to attack if machines and auditors are selected and assigned in a publicly transparent and random manner.

Conclusions about Taking Action When Anomalies Are Found in the Automatic Routine Audit

As is the case for DREs w/VVPT, an Automatic Routine Audit of PCOS ballots offers questionable security benefit unless effective procedures to investigate discrepancies (including taking remedial action, where necessary) are implemented and adhered to. Detection of possible fraud without an effective response will not thwart an attack on voting systems. For further discussion of this topic, *see supra* pp. 74–75.

PREVENTION OF WIRELESS COMMUNICATION: A POWERFUL COUNTERMEASURE FOR ALL THREE SYSTEMS

Against all three systems, attackers could use wireless components to subvert *all* testing.

As already discussed in some detail (*see supra* pp. 46, 48, 55–56), our analysis shows that machines with wireless components are particularly vulnerable to Trojan Horse and other attacks. We conclude that this danger applies to all three systems we have examined. Only two states, New York and Minnesota, ban wireless components on all machines.[186] California's ban on wireless components appears to apply to DREs only.[187]

Unfortunately, banning *use* of wireless components on voting systems without banning the wireless components themselves (as is done in several states) still poses serious security risks. First, a Software Attack Program could be designed to re-activate any disabling of the wireless component. In such circumstances, the voting machine might indicate that the wireless component was off, when it actually could receive signals. Second, pollworkers or anyone else with access to the voting machine could turn on the wireless component when it was supposed to be turned off. Under either scenario, our attacker could use a wireless-enabled PDA or other device to send remote signals to the wireless component and install her attack.

Vendors continue to manufacture and sell machines with wireless components.[188] Among the many types of attacks made possible by wireless components are attacks that exploit an unplanned vulnerability in the software or hardware to get a Trojan Horse into the machine. For this type of attack, an attacker would not need to insert a Trojan Horse in advance of Election Day. Instead, if she was aware of a vulnerability in the voting system's software or firmware, she could simply show up at the polling station and beam her Trojan Horse into the machine using a wireless-enabled PDA.

Thus, virtually any member of the public with some knowledge of software and a PDA could perform this attack. This is particularly troubling when one considers that most voting machines run on COTS software and/or operating systems; the vulnerabilities of such software and systems are frequently well known.[189]

Against all three systems, attackers could use wireless components to subvert *all* testing. Specifically, an attack program could be written to remain dormant until it received specific commands via a wireless communication. This would allow attackers to wait until a machine was being used to record votes on Election Day before turning the software attack on.

Attackers could also use wireless communications to gain fine-grained control over an attack program already inserted into a particular set of machines (*i.e.*,

switch three votes in the second race on the third machine), or obtain information as to how individuals had voted by communicating with a machine while it was being used.

Finally, wireless networking presents additional security vulnerabilities for jurisdictions using DREs w/VVPT and PCOS. A major logistical problem for an attacker changing both electronic and paper records is how to get the new paper records printed in time to substitute them for the old record in transit. With wireless networking, the DRE or PCOS can transmit specific information out to the attacker about what should appear on those printed records. In short, permitting wireless components on VVPT or PCOS machines makes the attacker's job much simpler in practice.

SECURITY RECOMMENDATIONS

There is a substantial likelihood that the election procedures and countermeasures currently in place in the vast majority of states would not detect a cleverly designed Software Attack Program.

There is a substantial likelihood that the election procedures and countermeasures currently in place in the vast majority of states would not detect a cleverly designed Software Attack Program. The regimens for Parallel Testing and Automatic Routine Audits proposed in the Security Report are important tools for defending voting systems from many types of attack, including Software Attack Programs. For the reasons discussed, *supra* pp. 6–7, we also believe that these measures would reduce the likelihood that votes would be lost as a result of human error.

Most jurisdictions have not implemented these security measures. Of the 26 states that require a voter-verified paper record, only 12 states require automatic audits of those records after every election, and only two of these states – California and Washington – conduct Parallel Testing.[190] Moreover, even those states that have implemented these countermeasures have not developed the best practices and protocols that are necessary to ensure their effectiveness in preventing or revealing attacks or failures in the voting systems.

Recommendation #1:
Conduct Automatic Routine Audit of Paper Records.

Advocates for voter-verified paper records have been extremely successful in state legislatures across the country. Currently, 26 states require their voting systems to produce a voter-verified record, but 14 of these states do not require Automatic Routine Audits.[191] The Task Force has concluded that an independent voter-verified paper trail without an Automatic Routine Audit is of questionable security value.[192]

By contrast, a voter-verified paper record accompanied by a solid Automatic Routine Audit can go a long way toward making the least difficult attacks much more difficult. Specifically, the measures recommended below should force an attacker to involve hundreds of informed participants in her attack.

- A small percentage of all voting machines and their voter-verified paper records should be audited.
- Machines to be audited should be selected in a random and transparent way.
- The assignment of auditors to voting machines should occur immediately before the audits. The audits should take place by 9 a.m., the day after polls close.
- The audit should include a tally of spoiled ballots (in the case of VVPT cancellations), overvotes, and undervotes.

For paperless DRE voting machines, Parallel Testing is probably the best way to detect most software-based attacks.

- A statistical examination of anomalies, such as higher-than-expected vote cancellations or over- and undervotes, should be conducted.
- Solid practices with respect to chain of custody and physical security of paper records prior to the Automatic Routine Audit should be followed.

Recommendation #2: Conduct Parallel Testing.

It is not possible to conduct an audit of paper records of DREs without VVPT because no voter-verified paper record exists on such machines. This means that jurisdictions that use DREs without VVPT do not have access to an important and powerful countermeasure.

For paperless DRE voting machines, Parallel Testing is probably the best way to detect most software-based attacks as well as subtle software bugs that may not be discovered during inspection and other testing. For DREs w/VVPT and ballot-marking devices, Parallel Testing provides the opportunity to discover a specific kind of attack (for instance, printing the wrong choice on the voter-verified paper record) that may not be detected by simply reviewing the paper record after the election is over. However, even under the best of circumstances, Parallel Testing is an imperfect security measure. The testing creates an "arms race" between the testers and the attacker, but the race is one in which the testers can never be certain that they have prevailed.

We have concluded that the following steps will lead to more effective Parallel Testing:

- The precise techniques used for Parallel Testing (*e.g.*, exactly how and when the machine is activated, how activation codes/smart cards/*etc.* are produced to allow voting, *etc.*) should not be fully determined or revealed until right before the election. Details of how Parallel Testing is done should change from election to election.
- At least two of each type of DRE (meaning both vendor and model) should be selected for Parallel Testing.
- At least two DREs from each of the three largest counties should be parallel tested.
- Localities should be notified as late as possible that machines from their precincts will be selected for Parallel Testing.
- Wireless channels for voting machines should be closed off to ensure they cannot receive commands.
- Voting machines should never be connected to one another during voting.[193]

- Voting machines should be completely isolated during the election, and print out or otherwise display their totals *before* being connected to any central server to send in its tallies.

- Parallel Testing scripts should include details such as how quickly or slowly to vote, when to make "errors," and perhaps even when to cast each vote.

- Parallel Testing should be videotaped to ensure that a contradiction between paper and electronic records when Parallel Testing is complete is not the result of tester error.

Machines with wireless components are particularly vulnerable to attack.

While a few local jurisdictions have taken it upon themselves to conduct limited Parallel Testing, we are aware of only three states, California, Maryland and Washington, that have regularly performed Parallel Testing on a statewide basis. It is worth noting that two of these states, California and Washington, employ Automatic Routine Audits *and* Parallel Testing as statewide countermeasures against potential attack.

Recommendation # 3:
Ban Wireless Components on All Voting Machines.

Our analysis shows that machines with wireless components are particularly vulnerable to attack. We conclude that this vulnerability applies to all three voting systems. Only two states, New York and Minnesota, ban wireless components on all machines.[194] California also bans wireless components, but only for DRE machines. Wireless components should not be permitted on any voting machine.

Recommendation # 4:
Mandate Transparent and Random Selection Procedures.

The development of transparently random selection procedures for all auditing procedures is key to audit effectiveness. This includes the selection of machines to be Parallel Tested or audited, as well as the assignment of auditors themselves. The use of a transparent and random selection process allows the public to know that the auditing method was fair and substantially likely to catch fraud or mistakes in the vote totals. In our interviews with election officials we found that, all too often, the process for picking machines and auditors was neither transparent nor random.

In a transparent random selection process:

- The whole process is publicly observable or videotaped.

- The random selection is to be publicly verifiable, *i.e.*, anyone observing is able to verify that the sample was chosen randomly (or at least that the number selected is not under the control of any small number of people).

- The process is simple and practical within the context of current election practice so as to avoid imposing unnecessary burden on election officials.

Recommendation # 5:
Ensure Local Control of Election Administration.

Where a single entity, such as a vendor or state or national consultant, runs elections or performs key tasks (such as producing ballot definition files) for multiple jurisdictions, attacks against statewide elections become easier. Unnecessary centralized control provides many opportunities to implement attacks at multiple locations.

Recommendation # 6: Implement Effective Procedures for Addressing Evidence of Fraud or Error.

Both Automatic Routine Audits and Parallel Testing are of questionable security value without effective procedures for action where evidence of machine malfunction and/or fraud is uncovered. Detection of fraud without an appropriate response will not prevent attacks from succeeding. In the Brennan Center's extensive review of state election laws and practices and in its interviews with election officials for the Threat Analysis, we did not find any jurisdiction with publicly detailed, adequate, and practical procedures for dealing with evidence of fraud or error discovered during an audit, recount or Parallel Testing.

The following are examples of procedures that would allow jurisdictions to respond effectively to detection of bugs or Software Attack Programs in Parallel Testing:

- Impound and conduct a transparent forensic examination of all machines showing unexplained discrepancies during Parallel Testing.
- Where evidence of a software bug or attack program is subsequently found (or no credible explanation for the discrepancy is discovered), conduct a forensic examination of all DREs in the state used during the election.[195]
- Identify the machines that show evidence of tampering or a software flaw that could have affected the electronic tally of votes.
- Review the reported margin of victory in each potentially affected race.
- Based upon the (1) margin of victory, (2) number of machines affected, and (3) nature and scope of the tampering or flaw, determine whether there is a substantial likelihood that the tampering or flaw changed the outcome of a particular race.

- Where there is a substantial likelihood that tampering changed the outcome of a particular race, hold a new election for the office.

The following is an illustrative set of procedures that would allow jurisdictions to respond effectively to discrepancies between paper and electronic records during an Automatic Routine Audit:

- Conduct a transparent investigation of all machines where the paper and electronic records do not match to determine whether there is any evidence that tampering with the paper records has occurred.
- To the extent that there is no record that the paper records have been tampered with, certify the paper records.
- If there is evidence that the paper records have been tampered with, give a presumption of authority to the electronic records.
- After giving a presumption of authority to the electronic records, conduct a forensic investigation on all machines where the paper and electronic records do not match to determine whether there has been any tampering with the electronic records.
- If tampering with the electronic records can be ruled out, certify the electronic records.[196]
- Where there is evidence that both sets of records have been tampered with, conduct a full recount to determine whether and to what extent paper and electronic records cannot be reconciled.
- At the conclusion of the full recount, determine the total number of machines that report different electronic and paper records.
- After quantifying the number of machines that have been tampered with, determine the margin of victory in each potentially affected race.
- Based upon (1) the margin of victory, (2) the number of machines affected, and (3) the nature and scope of the tampering, determine whether there is a substantial likelihood that tampering changed the outcome of a particular race.
- In the event that a determination is made that there is a substantial likelihood that tampering changed the outcome of a particular race, hold a new election for the office.

Election officials and voting systems experts should be looking at ways to ensure that voters understand their role in creating a more secure voting system.

DIRECTIONS FOR THE FUTURE

We are hopeful that this report will spur further orderly and empirical analyses of threats to voting systems for the purpose of assessing new voting systems as well as proposed security procedures and countermeasures. Some of our suggestions for further study are detailed below.

WITNESS AND CRYPTOGRAPHIC SYSTEMS

This report was necessarily limited to analyzing systems currently in use. Further security analyses must be performed on witness and cryptographic voting systems, which provide some hope of offering election officials additional choices for independently verifiable voting systems in the future.

For a detailed discussion of these systems and their potential, *see* the website of the Electronic Privacy Information Center at http://www.epic.org/privacy/voting/eac_foia/v1ad.doc. Also *see* the website of the Society for Industrial and Applied Mathematics at http://www.siam.org/siamnews/04-04/voting.pdf.

INFORMING VOTERS OF THEIR ROLE IN MAKING SYSTEMS MORE SECURE

This report makes clear that informed voters are an important defense against potential attacks. The larger the number of voters who check their VVPT before casting their vote, the less likely that an Automatic Routine Audit would be unable to catch a Trojan Horse attack. Similarly, the more voters who fill out their PCOS ballots correctly, the less likely that a Trojan Horse attack on the over/undervote protection or scanner calibration will affect the number of recorded votes.

Election officials and voting systems experts should be looking at ways to ensure that voters understand their role in creating a more secure voting system.

ADDITIONAL STATISTICAL TECHNICAL TECHNIQUES TO DETECT FRAUD

This study has pointed to at least two areas where statistical techniques in the Automatic Routine Audit could be used to catch fraud: (1) where there is an unusually high number of cancellations on the VVPT, and (2) where there is an unusually high number of over/undervotes on PCOS ballots. We encourage statisticians and political scientists to find additional statistical techniques to detect fraud.

LOOKING FOR BETTER PARALLEL TESTING TECHNIQUES

We conclude that Parallel Testing can be a useful countermeasure that should make voting systems more secure, particularly in jurisdictions where voting systems do not have voter-verified paper records. We have made a number of observations concerning solid Parallel Testing practices. We believe that additional studies should be done to attempt to make Parallel Testing practices even stronger. Parallel Testing creates an "arms race" of sorts between the testers and the attacker – where the testers can never be certain that they have prevailed.

LOOKING AT OTHER ATTACK GOALS

This report took on the simplifying assumption that the attacker's objective was to change the outcome of a statewide race. But attackers could have other goals: to attack voter privacy, disrupt an election, or discredit the electoral process. All of these are serious threats that we should guard against. Methodical threat analyses of these attack objectives would also be useful and employing the same approach used here might well provide critical insight.

LOOKING AT OTHER RACES

The method and analysis of this study can be applied to any race, real or hypothetical, local or statewide.[197] We encourage security analysts, public officials and interested citizens to use the information and methods in this document to address their specific security concerns.

GLOSSARY[198]

Automatic Routine Audit. Automatic Routine Audits are used in twelve states to test the accuracy of electronic voting machines. They generally require that between 1 and 10% of all precinct voting machines be audited.[199] The Task Force findings regarding Automatic Routine Audit regimens can be found in this report at pages 76–77, and 87–88.

Cryptic or Secret Knock. Where a Trojan Horse or other Software Attack Program has been inserted into a machine, a Cryptic Knock is an action taken by a user of the machine that will trigger (or silence) the attack behavior. The Cryptic Knock could come in many forms, depending upon the attack program: voting for a write-in candidate, tapping a specific spot on the machine's screen, a communication via wireless network, *etc.*

Configuration Files. Voting systems are generally designed to be used across many jurisdictions with very different needs, regulations and laws. In addition to the ballot definition information in a voting terminal on Election Day, there are a wide range of settings that must be configured correctly in order to be have the terminal perform correctly. For instance, machines must be configured to tell the system how to behave when a voter leaves with a ballot not completed and the election officials indicate to the machine that the voter has left without casting his ballot. In some jurisdictions, the machine should cast the ballot while in others, it should void the ballot. These settings can be thought of as residing in configuration files, although they may actually be stored in the Windows Registry, in a database or elsewhere.

Driver. In general, a driver is a program designed to interface a particular piece of hardware to an operating system or other software. Computer systems are designed with drivers so that many programs such as MS Word, QuickBooks, and Firefox web browser, for example, could interface with lots of devices such as printers, monitors, plotters, and barcode readers without having to have each one of these programs depend on the details of each device. With regard to voting technology, drivers are likely to be present to interface with audio devices for accessibility, the screen, the touch-screen hardware, a printer for printing totals and other information, and for interfacing with the battery backup unit.

Event and Audit Logs. In general, computer systems are programmed to record all activities that occur, including when they are started up, when they are shut down, *etc.* A voting terminal could be programmed to remember when it was started, shutdown, when it printed its zero tape, and the like. Such records are Event Logs or Audit Logs. These records could be helpful during a forensic analysis of voting systems after a suspected attack.

Independent Testing Authority. Starting with the 1990 FEC/NASED standards, independent testing authorities ("ITAs") have tested voting systems, certifying

that these systems meet the letter of the "voluntary" standards set by the federal government and required, by law, in most states. Several states, such as Florida, that impose additional standards contract with the same labs to test to these stronger standards.[200]

Logic and Accuracy Testing (or "L&A" Testing). This is the testing of the tabulator setups of a new election definition to ensure that the content correctly reflects the election being held (*i.e.,* contests, candidates, number to be elected, ballot formats, *etc.*) and that all voting positions can be voted for the maximum number of eligible candidates and that results are accurately tabulated and reported.[201] Logic and Accuracy Testing should not be confused with Parallel Testing. Logic and Accuracy Testing is generally done prior to the polls opening; it is not intended to mimic the behavior of actual voters and generally lasts only a few minutes. Most machines have a "Logic and Accuracy" setting so that the machine "knows" it is being tested.

Parallel Testing. Parallel Testing, also known as election-day testing, involves selecting voting machines at random and testing them as realistically as possible during the period that votes are being cast. The Task Force findings regarding Parallel Testing regimens can be found in this report *supra* pp. 52–59 and 88–89.

Software Attack Program. Any destructive program, including Trojan Horses, viruses or other code, that is used to overtake voting systems for the purpose of altering election results.

Trojan Horse. A destructive program that masquerades as a benign program. Unlike viruses, Trojan Horses do not replicate themselves.

ENDNOTES

[1] Ballot Marking Devices have been purchased by several jurisdictions in recent months. However, they have not yet been purchased as the primary machine in any jurisdiction's voting system. Instead, they have generally been purchased as the "accessible" unit, to meet the Help America Vote Act's accessibility requirements. Lawrence Norden, *Voting System Usability in* THE MACHINERY OF DEMOCRACY (Brennan Center for Justice ed., forthcoming July 2006).

[2] These systems are currently used to a limited extent in both Vermont and New Hampshire. Lawrence Norden *et al., Voting System Accessibility, in* THE MACHINERY OF DEMOCRACY (Brennan Center for Justice ed., forthcoming July 2006).

[3] These systems are currently in development and not commercially available. They are discussed in further detail *infra* p. 92.

[4] In 2004, 27 States allowed early voting. Approximately 19.3% of voters in these states voted early. Approximately 11.6% of votes counted in 2004 were absentee ballots. Oregon is the only state with an all-mail voting system. *See* Election Assistance Commission, *EAC Election Day Survey,* http://www.eac.gov/election_survey_2004/statedata/StateLevelSummary.htm (turnout source tab at bottom) (Last visited May 25, 2006).

[5] These reports will be released under separate cover in 2006. *See supra* notes 1 and 2 and *infra* note 184.

[6] NIST has informed the Brennan Center that the development of policy recommendations for voting systems is not within the agency's mission or institutional authority. Accordingly, the policy recommendations in the report should not be attributed to Task Force members who work for NIST.

[7] Tracy Campbell, DELIVER THE VOTE, at xvi (2005) (pointing to, among other things, a history of vote buying, ballot stuffing, and transposing of results).

[8] *Id.*

[9] Joseph P. Harris, ELECTION ADMINISTRATION IN THE UNITED STATES (1934).

[10] *See e.g.* DELIVER THE VOTE, *supra* note 7 at 275-284; Edmund F. Kallina, Jr., COURTHOUE OVER WHITE HOUSE – CHICAGO AND THE PRESIDENTIAL ELECTION OF 1960 (1988) (documenting fraud found in Chicago's 1960 elections); Andrew Gumbel, STEAL THIS VOTE, at 173-200 (2005) (detailing tampering and questionable results in the era of lever and punch-card voting).

[11] DELIVER THE VOTE, *supra* note 7 at 83, 99, 137.

[12] *See, e.g., Chip Glitch Hands Victory to Wrong Candidate,* ASSOCIATED PRESS, Nov. 11, 2002 (noting that a "defective computer chip in [Scurry] County's optical scanner misread ballots . . . and incorrectly tallied a landslide victory for Republicans.")

[13] *See, e.g., Computer Loses More Than 4,000 Early Votes in Carteret,* CHARLOTTE OBSERVER, Nov. 4, 2004 (noting that as a result of a software bug, machines could only store 3,005 votes; after this number of votes was recorded the machines accepted, but did not store, the ballots of 4,438 voters in the 2004 presidential election).

[14] *See, e.g.,* Anna M. Tinsley and Anthony Spangler, *Vote Spike Blamed on Program Snafu,* FORT WORTH STAR-TELEGRAM, Mar. 9, 2006, (noting that a programming error in the tally server software caused an extra 100,000 votes to be initially recorded in Tarrant County, Texas).

[15] *See, e.g.,* Susan Kuczka, *Returns Are In: Software Goofed – Lake County Tally Misled 15 Hopefuls,* CHICAGO TRIBUNE, Apr. 4, 2003, at 1 (noting that programming error caused machines to record names of wrong candidates).

[16] *See, e.g., Voters Turned Away After Waiting Hours* (WPLG Local 10 News television broadcast,

Nov. 1, 2004) (noting that breakdowns of DREs in Broward County forced people to wait to vote for hours before they could vote), available at http://www.local10.com/news/3878344/detail.html.

17 *See, e.g.*, Kevin P. Connolly, *Computer Glitches Slow Volusia Results: County Officials Ask the Machine's Supplier to Investigate Why Memory Cards Failed Tuesday*, ORLANDO SENTINEL, Nov. 4, 2004 at A17.

18 *Nearly 40 Votes May Have Been Lost in Palm Beach County*, USA TODAY, Nov. 2, 2004, at B7 (noting that failure to properly plug in machine appeared to cause the loss of as many as 40 votes).

19 Douglas W. Jones, *Threats to Voting Systems* at 2 (Oct. 7, 2005), *available at* http://vote.nist.gov/threats/papers/threats_to_voting_systems.pdf (presented at the NIST Threat Analysis Workshop).

20 The catalogs are available at www.brennancenter.org [hereinafter *Attack Catalogs*].

21 We determined that looking at each attack in the context of an effort to change a statewide election was critical to determining its difficulty. There are many ways to switch or spoil a single vote. It would be impossible for election officials to guard against all such threats. The challenge is to prevent those attacks that (a) are feasible, and (b) if carried out successfully would affect a large number of votes. By looking at attacks that could affect statewide elections, we have attempted to limit ourselves to these types of attacks.

22 *See, Attack Catalogs, supra* note 20.

23 The specifics might differ slightly. A vote buying scheme against DREs or DREs w/VVPT could involve the use of a small camera, whereby the voter would photograph the confirmation screen or VVPT to prove that she voted the way she promised. This would not work in the case of a PCOS vote, as there is no display confirming the voter's intention. To merely take a picture of the PCOS ballot would prove nothing – the voter could photograph a ballot that showed she voted for Johnny Adams, but erase that vote and submit her ballot marked for Tom Jefferson. *See* Attack Number 26 in the DRE w/VVPT Catalog and Attack Number 26 in the DRE Catalog, *Attack Catalogs, supra* note 20.

24 Of course, statewide elections are occasionally decided by mere dozens or hundreds of votes. But these are the exceptions among the exceptionally close races. As discussed in more detail, *infra* pp. 20–23, we have assumed that in attempting to affect a close statewide race, an attacker must presume that one candidate's margin of victory will be somewhere from 2–3% of all votes.

25 *See* PCOS Attack Catalog, *Attack Catalogs, supra* note 20.

26 In assigning values, we have made certain assumptions about the jurisdiction's security measures. As discussed in greater detail, *infra* pp. 14–15, these assumptions are based upon survey responses from and interviews with current and former election officials about their security practices. Among the assumptions we have made: (1) at the end of an Election Day, but prior to the transportation of ballots, poll workers check the total number of votes cast against the poll books in each polling place, and (2) ballots from each polling place are delivered to central county offices separately (*i.e.*, a single person or vehicle does not go from polling place to polling place collecting ballots before delivering them to the central location).

27 This number was reached after considering the total number and types of ballots that would have to be stolen or created.

28 Given the difficulty of stuffing the ballot box and modifying poll books, we have assumed that at least one person would be needed for each task in every polling place where it is accomplished. Of course, there is a real possibility that if this attack were carried out, someone would get caught. At the very least, stuffing the ballot box and modifying the ballot boxes *in the polling place* would be difficult to do without attracting notice. If anything, this fact supports our methodology. It is not impossible to imagine that, with the proper motivation and skills, two people could accom-

plish these goals in a single polling place somewhere in the country. It is far more difficult to imagine dozens or hundreds of people accomplishing this task successfully in dozens or hundreds of polling places in the same state. For this reason, and under our methodology, the attack is labeled "very difficult" to accomplish successfully.

[29] Among those interviewed in July and Aug. of 2005 regarding the difficulty of various attacks on election systems were Debbie Smith, Elections Coordinator, Calaveras County, CA; Patrick F. Gill, Auditor, Sioux City, IA; Wendy Noren, County Clerk of Boone County, MO; Beverly J. Harry, County Clerk/Registrar of Voters, Inyo County, CA ; Larry Lomax, Registrar of Voters, Clark County, NV; Cliff Borofsky, Election Administrator for Bexar County, TX; F. Robert Williams, Chief Information Officer for Monmouth County, NJ; and Brian Newby, Election Commissioner of Johnson County, KS.

[30] Wikipedia, *US Senate Election, 2000*, http://en.wikipedia.org/wiki/U.S._Senate_election,_2000 (as of May 25, 2006, 15:30 GMT).

[31] International Information Programs, *2004 U.S. Elections Results Finally Complete*, http://usinfo.state.gov/dhr/Archive/2005/Jan/03-462014.html (Dec. 30, 2004).

[32] Zogby International, *Election 2004 Zogby Battleground State Polls, at* http://www.zogby.com/news/ ReadNews.dbm?ID=904 (Oct. 24, 2004).

[33] While our results are derived from a review of a composite election in a composite jurisdiction, we believe they are applicable to similarly close elections in almost any state. As a check on our findings, we have run an analysis of Attack Catalogs against the Presidential race in Washington State in 2004, and come up with substantially similar results to those discussed in this paper.

[34] Steganography is "the art and science of writing hidden messages in such a way that no one apart from the intended recipient knows of the existence of the message." Wikipedia, *Steganography*, http://en.wikipedia.org/wiki/Steganography (as of May 25, 2006, 15:33 GMT).

[35] *See infra* note 121.

[36] Responses to the Brennan Center Security Survey are on file at the Brennan Center. For a sample survey, *see* Appendix D.

[37] Starting with the 1990 FEC/NASED standards, Independent Testing Authorities ("ITAs") have tested voting systems, certifying that these systems meet the letter of the "voluntary" standards set by the federal government and required, by law, in most states. Several states, such as Florida, that impose additional standards contract with the same labs to test to these stronger standards. In the future, the EAC will be in charge of certification that will be done by VSTLs (Voting System Test Labs). For further explanation of this change, *see* Election Assistance Commision, *Voluntary Voting System Guidelines* (2005), *available at* http://www.eac.gov/VVSG%20Volume_II.pdf (Last visited May 31, 2006). For further discussion of the testing most machines undergo, *see* Appendix E.

[38] Our analysis shows that this is a very important countermeasure. Specifically, this countermeasure allows pollworkers and the public to ensure that corrupt or flawed software on a county's central tally-server does not incorrectly add up machine vote totals.

[39] A thorough discussion of the types of testing voting machines might be subject to is provided in Appendix E.

[40] We have assumed that each machine delivered by a vendor to the jurisdiction is tested by that jurisdiction. Even if the vendor has some kind of quality control guarantees, these are of no value unless the customer detects failures at the time of delivery. At minimum, such tests would include power-on testing, basic user interface tests (do all the buttons work, does the touch-screen sense touches at all extremes of its surface, do the paper-feed mechanisms work, does the uninterruptible power supply work). This is known as "Acceptance Testing." For a more detailed discussion of Acceptance Testing, *see* Appendix E.

[41] We have assumed that before each election every voting machine would be subject to public testing. This is frequently described as Logic and Accuracy testing or simply L&A testing, a term that is more appropriate in the realm of punch-card and mark-sense ballot tabulating machines than in the realm of DRE systems, but the term is used widely and in many states it is enshrined in state law. For a more detailed discussion of Logic and Accuracy testing, *see* Appendix E.

[42] Electionline.org, *Recounts: From Punch Cards to Paper Trails*, at 3 (Oct. 2005) [hereinafter *Recounts*], at http://www.electionline.org/Portals/1/Publications/ERIPBrief12.SB370updated.pdf (Last visited May 25, 2006).

[43] California selects auditors at the county level by political party. Telephone Interview by Eric L. Lazarus with Debbie Smith, Elections Coordinator, Calaveras County, CA (July 14, 2005). We assume each audit team will have at least two members, with one member selected by each political party.

[44] This might be difficult in the selection of machines for Parallel Testing. If election officials insist on one-month's notice as to which precincts will be tested, publication of the selected machines could be problematic. Specifically, this would allow an attacker to know which precincts to avoid attacking.

[45] Many more recommendations for a sound Parallel Testing regime can be found in the subsection entitled "Effects of Regimen for Parallel Testing," *infra* pp. 52–59.

[46] In California election officials generally felt they needed at least a month's notice – this is because when Parallel Testing is done, certain precincts will lose the use of one or two machines. Telephone interview by Eric L. Lazarus with Jocelyn Whitney, Developer and Project Manager for Parallel Testing in California (Dec. 23, 2005).

[47] In a threat paper entitled *"Trojan Horse in DRE -OS"* posted by Chris Lowe for the NIST Threat Analysis Workshop in Oct. 2005, Mr. Lowe imagined an attack in an election involving Tom Jefferson and John Adams. The analysis in this paper should not be confused with Mr. Lowe's work, although we do reference Mr. Lowe's threat paper, *infra* note 120.

[48] Because this report does not address security issues related to absentee voting, and for purposes of simplicity, we are assuming that all votes were cast at a polling place on one of the three voting systems we are examining.

[49] The numbers in this appendix represent the average number of polling places and precincts in the three largest counties in each of the Zogby battleground states in 2004 presidential election (*see supra* note 32). Milwaukee County was not included in this analysis because they divide up polling places and precincts in a way that made comparison impossible.

[50] If an attacker were to switch 4% of the votes from Candidate A to Candidate B, it would have the same effect on the margin of victory as adding 8% of the total votes to Candidate A, or subtracting 8% of the total votes from candidate B. This can be demonstrated in a simple example. Suppose Candidate A and Candidate B each received 50 votes. If we switched 4 votes from Candidate B to Candidate A, Candidate A would win the election by 8 votes: 54 for Candidate A, 46 for Candidate B. If on the other hand, we simply stuffed the ballot box and added 8 votes for Candidate A, but did not otherwise tamper with the election results, Candidate A would again win by 8 votes: 58 votes for Candidate A, and 50 votes for Candidate B.

[51] This assumes that the county does not post PDF images of the ballot on the web prior to the election; this was done by, among other counties, St. Lucie County, Florida prior to the General Election of 2000.

[52] *See also* Appendix G.

[53] This analysis does not even consider how much *more* difficult the attack would become if one of our two other sets of countermeasures was in place. For instance, under the Basic Set of

Countermeasures, "ballot boxes are examined (to ensure they are empty) and locked by poll workers immediately before the polls are opened." This simple countermeasure would make PCOS Attack 12 significantly more difficult to execute successfully; the attackers could not simply scan ballots just before Election Day and hope that these ballots would become part of the tally. They would have to co-opt every person charged with reviewing the ballot boxes prior to opening in all 606 targeted polling places.

54 Cook County Election Department, *Results from November 2004 Elections, at* http://www.voterinfonet.com/results/detail/summary.php?election=20041102G (Last visited May 31, 2006).

55 Of course, it is possible that an attacker could switch more than this percentage of votes in a single machine, polling place or county without detection. To the extent that she could do so, her ability to successfully change the outcome of a statewide election would be made easier. For a complete list of assumptions made about Pennasota, *see* Appendix G.

56 As discussed in greater detail, *infra* p. 72, for some attack scenarios, the ability to carry out the attack in the fewest possible counties is key to (a) involving the fewest number of informed participants and (b) increasing the chances that the attack will not be detected. In other scenarios, a statewide attack is more likely to accomplish these goals.

57 Specifically, our attacker would need to add or subtract less than six percent (6%) of votes in these three counties; this means she would need to "switch" (*i.e.*, move a vote from one candidate to another) less than three percent (3%) of votes in these counties.

58 Based upon composite results from the three largest counties in each of the ten Zogby Battleground States reviewed, *See Zogby, supra* note 32.

59 The fact that we list these categories of attacks does not mean that we necessarily believe an attacker could successfully use these attacks to affect the outcome of our statewide election. We have concluded that some attacks would certainly fail if attempted. In such cases, the *Catalogs* label such attacks "N/A" under the column "Number of Informed Participants."

60 By "very difficult" we mean that it would require hundreds or thousands of informed participants; or, regardless of how many participants are involved, it would not affect enough votes to change the outcome of a close statewide race.

61 Dr. Michael Shamos, *Paper Trail Boycott* (Oct. 5, 2005) (a NIST Threat Analysis workshop presentation summarizing the logistics of this attack). A more detailed description of the attack can be found at http://vote.nist.gov/threats/papers/papertraiboycot.pdf.

62 This number is a high estimate. *See* Professor Benjamin Highton, *In Long Lines, Voting Machine Availability and Turnout*, 39 POLITICAL SCIENCE AND POLITICS 65, 67 (2006) (estimating that long lines in Franklin County, Ohio resulted in a 7.7% reduction in turnout in certain very large precincts).

63 There are 2,969 polling places in Pennasota. *See* Appendix G.

64 This section of the report borrows and relies heavily on *"Strategies for Software Attacks on Voting Machines,"* a white paper presented by John Kelsey of NIST at the NIST Threat Analysis workshop in Oct. 2005. This section does not cover the technical details and challenges of creating a successful software attack program in the same detail as Mr. Kelsey's paper. That paper can be found at http://vote.nist.gov/threats/papers/stategies_for_software_attacks.pdf.

65 *See* Computer Crime Research Center, *Report America Under Attack, at* http://www.crimeresearch.org/news/2003/04/ Mess0301.html (Last visited May 31, 2006) (noting a record number of computer hackers attacking military and government systems); *see also* Scott A. Boorman and Paul R. Levitt, *Deadly Bugs*, CHICAGO TRIBUNE (MAGAZINE) May 3, 1987 at C19 (detailing, among other attacks, the planting of a software bug in the computer system of the Los Angeles Department of Water and Power in 1985, which made some of the utilities' important internal files inaccessible for a week); Edward Iwata, *Companies Stress Network Security*, USA TODAY, Oct. 2, 2001

at 3B (citing "security audits" by security firm Sanctum in which they successfully broke "into the networks of 300 organizations, including federal agencies, financial firms and airlines").

66 *See* John Deutch *Off Line: At War with the Info-Terrorists,* THE OBSERVER, July 7, 1996 at 7 (the former Director of the Central Intelligence Agency cites attacks on computers and software to divert funds from banks, embezzle funds and commit fraud against credit card companies); L.A. Lorek, *Internet Worm Disrupts Business,* SAN ANTONIO EXPRESS-NEWS (Texas), Jan. 28, 2003 at 1E (discussing "Slammer," a computer worm which attacked a hole in Microsoft software and prevented banks and airlines from performing basic operations).

67 There is an extensive history of successful attacks against content protection systems, such as those created to protect digital media. *See generally* Wikipedia, *Digital Rights Management,* http://en.wikipedia.org/wiki/Digital_rights_management (detailing many such attacks) (as of May 26, 2006 15:39 GMT). For instance, in Oct. 1999 a teenaged Scandinavian high school dropout, Jon Lech Johansen, broke a much heralded DVD encryption scheme. *See* Wikipedia, *Content-Scrambling System,* http://en.wikipedia.org/wiki/Content_Scrambling_System (as of May 26, 2006 15:39 GMT).

68 Special purpose cryptographic devices are created to protect key material, even when an attacker has control over the device doing the encryption. There have been a number of successful attacks against such devices. *See* Ross Anderson, Mike Bond, Jolyon Clulow & Sergei Skorobogotav, *Cryptographic Processors – A Survey,* UNIVERSITY OF CAMBRIDGE COMPUTER LABORATORY TECHNICAL REPORT NO. 641 (Aug. 2005), at http://www.cl.cam.ac.uk/TechReports/UCAM-CL-TR-641.pdf, for an excellent history of some of these high-level attacks.

69 *See e.g.,* Jaikumar Vijayan, *Security Product Flaws are Magnets for Attackers,* COMPUTER WEEKLY, *at* http://www.computerweekly.com/Articles/Article.aspx?liArticleID=201449&PrinterFriendly=true (Mar. 29, 2004) (noting the growing number of attacks against "the very products users invest in to safeguard their systems").

70 For an example of this type of attack, see the discussion of Ron Harris's attack on video poker machines, *infra* note 148.

71 Domain Name System (DNS) is a distributed database that stores mappings of Internet Protocol addresses and host names to facilitate user-friendly web browsing. *See* Ian Betteridge, *Security Company Warns About DNS Attacks,* eWeek.com *at* http://www.eweek.com/article2/0,,1782543,00.asp, (Apr. 5, 2005) (for discussion of DNS attacks).

72 Dennis Callaghan, *Federal Sweep Nets Spammers, Cyber-Criminals,* eWeek.com, *at* http://www.eweek.com/print_article2/0,1217,a=134159,00.asp, (Aug. 26, 1994) (noting that the U.S. Department of Justice announced "that it has taken action against more than 150 individuals" accused of phishing and other related spam attacks); *2004: Year of the Cyber-Crime Pandemic,* eWeek.com, *at* http://www.eweek.com/article2/0,1895,1745848,00.asp (Jan. 1, 2005) (noting that between July and Nov. 2004, there was an average monthly growth rate of unique phishing attacks of 34%).

73 *See* Lisa Vaas, *No One-Stop Shopping to Stop Database Pilferages,* eWeek.com, *at* http://www.eweek.com/article2/0,1895,1904527,00.asp (Dec, 29, 2005) (describing attack on database of role-playing game company where attackers "exploited a software flaw and threatened to post stolen user data including user names, e-mail addresses and encrypted passwords" unless they were paid).

74 Bob Keefe, *New Worm is Thief, Not Prankster,* THE ATLANTA JOURNAL CONSTITUTION, Aug. 20, 2005 at 1G (detailing how criminals exploited a vulnerability in Microsoft software to "quietly 'harvest' ... sensitive data on a small number of computers – employee Social Security numbers, credit card numbers, passwords" – and then turn the machines into networks of "bots," to be "sold on virtual black markets").

75 Gavin Clarke, *Windows beats Linux-Unix on Vulnerabilities – CERT,* at http://www.theregister.

co.uk/2006 /01/05/windows_linux_unix_security_vulnerabilities (Jan. 5, 2006).

[76] Brian Krebs, *Windows Security Flaw is 'Severe,'* WASHINGTON POST, Dec. 30, 2005 *at* D1.

[77] U.S. Government Accountability Office, *Elections: Federal Efforts to Improve Security and Reliability of Electronic Voting Systems Are Under Way, But Key Activities Need to Be Completed,* at 29 (Sept. 2005) (Report No. GAO-05-956) [hereinafter GAO Report] *available at* http://reform.house.gov/UploadedFiles/GAO-05-956.pdf.

[78] Brendan I. Koerner, *Welcome to the Machine,* HARPER'S MAGAZINE Apr. 1, 2004, at 83.

[79] *Id.; See also* Wikipedia entry for *Ron Harris,* http://en.wikipedia.org/wiki/Ron_Harris_(programmer) (as of May 30, 2006 15:00 GMT).

[80] In computing, "a patch is a small piece of software designed to update or fix problems with a computer program. This includes fixing bugs, replacing graphics and improving the usability or performance." *See* Wikipedia, *Software Patch,* http://en.wikipedia.org/wiki/Software_patch (as of May 26, 2006 15:42 GMT). Also *see* J. G. Levine *et. al., Detecting and Categorizing Kernel-Level Rootkits to Aid Future Detection,* IEEE SECURITY AND PRIVACY, Jan-Feb 2006, at 24-32.

[81] On a ballot (whether electronic or paper), candidate names are listed numerically with, say, "1" next to Tom Jefferson's name and "2" next to Johnny Adams. In the ballot definition file, programmers define what those numbers mean so when a voter touches a box next to 1 on the screen, the vote gets tallied for Tom Jefferson.

[82] This is not intended to be an exhaustive list.

[83] *GAO Report, supra* note 77 at 33.

[84] "A rootkit is a set of software tools frequently used by a third party (usually an intruder) after gaining access to a computer system. These tools are intended to conceal running processes, files or system data, which help an intruder maintain access to a system without the user's knowledge. Rootkits are known to exist for a variety of operating systems such as Linux, Solaris and versions of Microsoft Windows. A computer with a rootkit on it is called a rooted computer. The word "rootkit" came to public awareness in the 2005 Sony CD Copyright protection controversy, in which SONY BMG music CDs placed a rootkit on Microsoft Windows PCs." Wikipedia, *Root Kit,* http://en.wikipedia.org/wiki/Root_kit (as of May 30, 2006 15:50 GMT).

[85] *See* Tadayoshi Kohno, Adam Stubbelfield, Aviel Rubin, and Dan S. Wallach, *Analysis of an Electronic Voting System* at 13-14 (Feb. 2004), *at* http://avirubin.com/vote.pdf (paper for the IEEE Symposium on Security and Privacy); Dr. Michael A. Wertheimer, RABA Technologies LLC, *Trusted Agent Report: Diebold AccuVote-TS System* at 8 *available at* http://www.raba.com/press/TA_Report_AccuVote.pdf (Jan. 2004) (report prepared for Department of Legislative Services, Maryland General Assembly, Annapolis, Md.), [hereinafter "RABA Report"].

[86] *GAO Report, supra* note 77 at 25.

[87] The five points of vulnerability listed here are not meant to be a complete list; rather they represent some of the most obvious points of attack.

[88] *See,* Harri Hursti and Eric Lazarus, *Replaceable Media on Optical Scan,* NIST *at* http://vote.nist.gov/threats/papers/ReplaceableMediaOnOpticalScan.pdf (Last visited May 31, 2006).

[89] Kim Zetter, *Diebold Hack Hints at Wider Flaws,* WIRED NEWS, Dec. 21, 2005 *available at* http://www.wired.com/news/politics/evote/0,69893-0.html.

[90] *Id.*

[91] "A Red Team exercise is designed to simulate the environment of an actual event, using the same equipment and procedures of the system to be evaluated." *RABA Report, supra* note 85 at 16.

92 Responses to the Brennan Center Security Survey are on file at the Brennan Center. For sample survey, *see* Appendix D.

93 *See e.g.* Dean Takahashi, *Cautionary Tales for Security Expert*, PROCESSOR, Mar. 25, 2003 *available at* http://www.processor.com/editorial/article.asp?article=articles%2Fp2712%2F03p12%2F03p12.asp&guid=&searchtype=&WordList=&bJumpTo=True (detailing the reporting of security expert Kevin T. Mitnick, who showed how three hackers successfully obtained an old video-poker machine, took it apart and deciphered its software; this allowed them to steal more than $1 million from Las Vegas casinos).

94 As a reminder, the ballot definition files are created after a machine and its software have been tested and inspected. The files are sent to local jurisdictions and allow the machine to (a) display the races and candidates in a given election, and (b) record the votes cast.

95 "Personal digital assistants (PDAs or palmtops) are handheld devices that were originally designed as personal organizers, but became much more versatile over the years. A basic PDA usually includes a date book, address book, task list, memo pad, clock, and calculator software. Many PDAs can now access the Internet via Wi-Fi, cellular or Wide-Area Networks (WANs) or Bluetooth technology. One major advantage of using PDAs is their ability to synchronize data with a PC or home computer." Wikipedia, *Personal Digital Assistant, at* http://en.wikipedia.org/wiki/Personal_digital_assistant (as of May 26, 2006 15:45 GMT).

96 A Cryptic Knock is an action taken by a user of the machine that will trigger (or silence) the attack behavior. The Cryptic Knock could come in many forms, depending upon the attack program: voting for a write-in candidate, tapping a specific spot on the machine's screen, a communication via wireless network, *etc.*

97 This is the testing of the tabulator setups of a new election definition to ensure that the content correctly reflects the election being held (*i.e.*, contests, candidates, number to be elected, ballot formats, *etc.*) and that all voting positions can be voted for the maximum number of eligible candidates and that results are accurately tabulated and reported.

98 For a more detailed discussion of specific attacks, *see* http://vote.nist.gov/threats or request a copy of the *Attack Catalogs* at www.brennancenter.org.

99 *RABA Report, supra* note 85, at 20-21.

100 A more complete description of the testing and inspection process for machines (touched upon *infra* pp. 42–44), can be found in Appendix E.

101 By "inspection" we mean review of code, as opposed to "testing," which is an attempt to simulate voting to ensure that the machine is functioning properly (and votes are being recorded accurately). We discuss testing in the next subsection.

102 David M. Siegel, an independent technology consultant for this report, contributed significantly to this subsection. For a more detailed discussion of the difficulty of catching attack programs through inspection, *see* Ken Thompson, *Reflections on Trusting Trust*, 27 COMMUNICATION OF THE ACM 761 (Aug. 1984), *available at* http://www.acm.org/classics/sep95.

103 This is a software program that is generally sold as commercial off-the-shelf software.

104 For further discussion of the limits of ITA testing and State Qualification Tests, *see GAO Report, supra* note 77 at 35; Douglas Jones's *"Testing Voting Machines", at* http://www.cs.uiowa.edu/~jones/voting/testing.shtml#ita (Last visited May 30, 2006); Dan S. Wallach, *Democracy at Risk: The 2004 Election in Ohio, Section VII: Electronic Voting: Accuracy, Accountability and Fraud,* DEMOCRATIC NATIONAL COMMITTEE VOTING RIGHTS INSTITUTE, at 4 (June 2005), *available at* http://www.votetrustusa.org/pdfs/ DNCElectronic%20Voting.pdf.

105 "Firmware is software that is embedded in a hardware device" (*i.e.*, the voting machine). Wikipedia, *Firmware, at* http://en.wikipedia.org/w/index.php?title=Firmware&oldid=48665273

(as of May 26, 2006 15:25 GMT).

106 Election Assistance Commission, *Voting Systems Standards Volume II, National Testing Guidelines* at §1.3.1.3, *available at* http://www.eac.gov/VVSG%20Volume_II.pdf (Last visited May 30, 2006).

107 *GAO Report, supra* note 77 at 35-36.

108 For a complete description of testing that a voting machine might be subject to, *see* Appendix E.

109 Some voters sign in but never vote (or finish voting). Thus, it might be possible to subtract votes from one candidate without altering the poll books and still prevent the attack from being noticed. An attacker would be limited, however, in the number of votes she could subtract from a candidate without raising suspicion.

110 In general, computer systems are programmed to record many activities that occur – including when they are started up, when they are shut down, *etc.* A voting terminal could be programmed to remember when it was started, shutdown, when it printed its zero tape, and the like. Such records are Event Logs or Audit Logs. Ordinarily, these records could be helpful during a forensic analysis of voting systems after a suspected attack.

111 This presupposes there is no paper record, or that if there is such a record, it is not reviewed.

112 Acronym for "basic input/output system." The BIOS is the built-in software that resides on a Read Only Memory Chip (ROM) that determines what a computer can do without accessing programs from a disk. Because the software is built-in to the machine, it is not subject to ITA inspection. It could both (a) contain an attack program and (b) delete entries from an Audit Log that might otherwise record the attack.

113 Independent investigators have already established that this is possible against multiple systems. As noted in the *GAO Report*, "Evaluations [have shown] that, in some cases, other computer programs could access ... cast vote files and alter them without the system recording this action in its audit logs." *GAO Report, supra* note 77 at 25. *See also* Compuware Corporation, *Direct Recording Electronic (DRE) Technical Security Assessment Report* at 42, (Nov. 2003) (prepared for the Ohio Secretary of State), *at* http://www.sos.state.oh.us/sos/hava/compuware112103.pdf; Harri Hursti, *The Black Box Report: SECURITY ALERT, Critical Security Issues with Diebold Optical Scan Design* at 18 (July 2005), at http://www.blackboxvoting.org/BBVreport.pdf; Michael Shamos, *UniLect Corporation PATRIOT Voting System: An Evaluation* at 11 (Apr. 2005) (paper prepared for the Secretary of the Commonwealth of Pennsylvania) *available at* http://www.house.gov/science/hearings/ets04/jun24/shamos.pdf.

114 Coordinating software attacks with paper records attacks is discussed in greater detail *infra* pp. 65–75.

115 This assumes an audit of the voter-verified paper record is conducted after voting is complete.

116 It is possible that an attack program could instruct a DRE printer to cancel votes and print false paper records to match attacked electronic records. This points to the importance of examining cancellations on VVPT printouts, as discussed *infra* pp. 65–71.

117 *See e.g.*, Kim Zetter, *Did e-Vote Firm Patch Election?*, WIRED NEWS Oct.13, 2003 (noting that employee of voting machine vendor claimed uncertified software patches were sent to election officials throughout Georgia to install just before the 2002 gubernatorial election) *available at* http://www.wired.com/news/politics/0,1283,60563,00.html; Andrew Orlowski, *California Set to Reject Diebold e-Voting machines* (Apr. 24, 2004) (noting that voting machine vendor sent software updates to voting machines in California just two weeks before the Presidential Primary in that state) *at* http://www.theregister.co.uk/2004/ 04/24/diebold_california.

[118] For a more detailed list of these potential attacks, as well as the steps and informed participant values assigned to them, *see* the "DRE without VVPT Catalog," *Attack Catalogs*, *supra* note 20.

[119] This summary borrows heavily from *"Trojan Horse in DRE -OS"* posted by Chris Lowe for the NIST Threat Analysis Workshop in Oct. 2005. A copy of that posting (which provides a more complete description of the attack) can be found *at* http://vote.nist.gov/threats/papers/TrojanHorse-DRE-OS.pdf.

[120] In fact, this is not a hypothetical scenario. We know that most voting systems run on commercially available operating systems. For instance, at least one major vendor runs its machines on a version of Micrsoft Windows called "CE." It is not difficult to imagine that one of the vendor's software developers could install such a Trojan Horse without detection.

[121] In this sense, this attack would not require the assistance of an "insider," such as a leading state or county election official.

[122] As already discussed, such updates and patches are issued on a fairly regular basis. For instance, on Jan. 6, 2006, Microsoft issued a patch to address a security flaw found in its operating system. John Fontana, *Microsoft Rushes out Patch for Windows Metafile Attack*, PC WORLD, Jan. 6, 2006 *available at* http://www.pcworld.com/news/article/0,aid,124246,00.asp.

[123] This assumes that the same DRE system is purchased by every county. Obviously, to the extent that the attackers wanted to attack more than one type of DRE system, they might need additional participants in their conspiracy.

[124] As already discussed, *supra* pp. 36–37, there are many ways for an attacker to gain such knowledge.

[125] Appendix G.

[126] Of course, few states use a single make and model of machine in every county. But even if a single DRE model represented 1 in 3 of all machines in the state, the attacker would need only target those machines and aim to switch between 4 and 6 votes per machine to affect tens of thousands of votes and change the results of the statewide election.

[127] In any event, even where code is subject to inspection, bad code can still get through. In separate instances in California and Indiana, election officials discovered that uncertified software had run on voting machines during elections. *See Marion County Election Board Minutes (Emergency Meeting)* at 7-18, (April 22, 2004) (Indiana) *available at* http://www.indygov.org/NR/rdonlyres/emkiqfxphochfss2s5anfuxbgj3zgpkv557moi3rb6f3ne44mcni2thdvoywyjcigyeoykwru53mopaa6kt2uxh7ofe/20040422.pdf; Office of the Secretary of State, *Staff Report on the Investigation of Diebold Elections System, Inc.* at 1-2 (Apr. 2004), (California) *at* http://www.ss.ca.gov/elections/ks_dre_papers/diebold_report_april20_final.pdf. In one case, the discovery was made when a vendor employee told a County Clerk; in the other, the uncertified software was revealed during a statewide audit of machines. We do not suggest that the software was installed to change the results of elections. Nevertheless, the fact that uncertified software ran on voting machines during elections, in violation of regulations and state law, demonstrates the difficulty of finding undesirable software on voting machines during inspection.

[128] Exactly what should happen when Parallel Testing finds that tested machines are misrecording votes is something that California (the only state to regularly perform parallel tests in the past) has not yet had to deal with. Obviously, merely finding corrupt software on a tested machine without taking further action will do nothing to thwart a software attack. Parallel Testing is much less likely to be an effective countermeasure if jurisdictions do not have in place clear procedures about what steps should be taken when the script and vote totals on a tested machine do not match.

[129] All of whom would have to be "insiders," in the sense that they would have had to have been chosen by the State or consulting group performing the Parallel Testing.

[130] *See* discussion in Appendix G.

[131] *Id.* This assumes that Pennasota uses the same make and model DRE in every precinct.

[132] *See* calculations in Appendix G.

[133] *Id.*

[134] Interview with Jocelyn Whitney, *supra* note 46.

[135] In fact, this is exactly how California has conducted its Parallel Testing; each Parallel Testing team casts 101 votes. *Id.*

[136] This is because to switch 51,891 votes, Trojan Horses will need to be activated on at least 2883 machines.

[137] *See* Appendix G.

[138] We calculate that a minimum of 61 attackers would be needed to subvert Parallel Testing in this way. The attackers could target 606 polling places in the three largest counties. It would be necessary for each attacker to get close enough to only ten polling places to transmit a wireless instruction to trigger the attack.

[139] Another possibility is that the Parallel Testers may always record the same number of votes. In previous elections in California, exactly 101 votes were processed during each Parallel Test. If the Trojan Horse is programmed to wait until the end of the election to switch votes, it could avoid all Parallel Testing by changing votes only where machines record more or less than 101 votes by the end of Election Day. E-mail from Jocelyn Whitney (Jan. 2, 2005) (on file with the Brennan Center).

[140] An alternative solution to the problem of creating a script that mirrors actual voter patterns would be to select volunteers, or "real" voters, to vote on the tested machines. These volunteers would be asked to vote as they normally would: this might create more realistic voting patterns without a script, but it potentially raises other privacy issues. We are not aware of any jurisdiction that currently performs Parallel Testing in this way.

[141] *Supra* note 135.

[142] E-mail from Office of the California Secretary of State to Eric L. Lazarus, Principal Investigator (Feb. 1, 2006) (on file with the Brennan Center).

[143] The Pennasota governor's race was designed to represent a closely contested statewide election. Our analysis shows that if a Trojan Horse were used to change just one vote per DRE, the result of the governor's race could be changed. In the case of such an attack, a successful Parallel Test would "detect" the misrecording of a single vote. Without a videotape of the testing itself, this misrecording could easily be misattributed to human error (*i.e.*, accidental deviation from the script). Even with video evidence, there may be a temptation to "explain away" such a discrepancy.

[144] Our total for the Parallel Testing set of countermeasures depends upon the ability of the attacker to create an Attack Program that can recognize if it is being tested. As already discussed, we believe that creating such an attack program would be technically and financially challenging – or would require the involvement of someone who was involved in or knew of the testing script – and have therefore agreed that it would probably require two additional conspirators. To the extent creating such an attack program is not feasible, the attack would require the subversion of at least 58 testers (who might be considered "insiders") to use a Cryptic Knock to shut off the Trojan Horse; we believe this would be very difficult to accomplish.

[145] For a more detailed list of these potential attacks, as well as the steps and informed participant values assigned to them, *see* the "DRE w/VVPT Catalog," *Attack Catalogs*, *supra* note 20.

[146] There are other potential entry points for parameterization: wireless communications and

Cryptic Knocks could also contain commands that tell voting machines when and how to attack a ballot.

147 Barbara Simmons, *Electronic Voting Systems: the Good, the Bad, and the Stupid*, The National Academy of Sciences, Computer Science and Technologies Board, at 7-8, *available at* http://www7.nationalacademies.org/cstb/project_evoting_simons.pdf (last visited May 30, 2006).

148 This attack is similar in structure to Ron Harris's attacks against computerized poker and other gaming machines (*see supra* p. 33): an employee with access to vendor software, hardware or firmware, inserts the Trojan Horse, which will not trigger until an accomplice sends commands.

149 *See* Appendix G. Based upon interviews with election officials in Nevada, we have concluded that DREs w/VVPT can handle slightly fewer voters per hour than DREs without VVPT. Accordingly we have estimated that Mega, Capitol and Suburbia county would have to have one DRE w/VVPT for every 120 voters.

150 *Recounts, supra* note 42 at 4. A few states, such as New Hampshire, have laws that allow for inexpensive, candidate initiative recounts. Attackers might be less inclined to target such states. The effect of these laws was not a subject of the Task Force analysis.

151 In fact, it would work exactly the same as any Software Attack Program against DREs, except that it would also target the VVPT to ensure that the paper records matched the electronic records.

152 Ted Selker and Sharon Cohen, *An Active Approach to Voting Verification* at 2 CalTech/MIT Voting Technology Project (May 2005), *at* http://vote.caltech.edu/media/documents/wps/vtp_wp28.pdf.

153 *Id.* at 5.

154 Given that many voters are likely to assume the mistake was their own, rather than the DRE's, we are skeptical that the number would be this high.

155 *See* Appendix G.

156 *Supra*, note 46.

157 Telephone interview with Larry Lomax, Registrar of Voters, Clark County, NV (Dec. 12, 2005).

158 There are 28,828 DREs w/VVPT in Pennasota. *See* Appendix G.

159 As detailed in Appendix A, we believe 606 polling places (in the three largest counties) is the minimum number of polling places the attacker could target and have a reasonable amount of certainty that she could still change the outcome of the election. If the attacker targeted 606 polling places, there would be approximately 22 more paper cancellations in these polling places than would otherwise be expected (13201/606=22).

160 *See* Appendix G.

161 If the attackers intercepted 550 convoys, there would still be 56 polling places with mismatching paper and electronic records. That represents roughly 0.2% of all polling places in the state. Under these circumstances, a 2% Automatic Routine Audit would still have a 66% chance of catching a mismatch. *See* Appendix K.

162 This is because our attackers seek to switch 51,891 votes. To avoid suspicion, they have not switched more than 15% of votes on any single DRE w/VVPT, which equals 18 (of 120) votes. 51,891/18=2,883.

163 For an explanation as to why nearly all of the paper rolls would need to be replaced in order to have a reasonable chance of avoiding detection during audit, *see* Appendix K.

164 According to the Department of Defense, these seals can cost as little as one or two cents

per seal; the Department of Defense estimates that for several models, it would take a knowledgeable and highly trained person at least several minutes to "defeat" each seal and gain access to the ballots. Telephone interview by Eric L. Lazarus with Mike Farrar, Department of Defense Lock Program, December 15, 2005. After defeating the thousands of seals, attackers would have to find a way to replace each one with a seal that looked exactly the same and contained the same unique number as the original.

165 If the employees assigned to guard the election materials are selected from a large pool of employees on-duty on election night, and if this selection process is done in a transparently random process just before the voter-verified paper records arrive at the county warehouse, the attacker would need to co-opt almost all of the larger pool to have a reasonable chance of co-opting the employees eventually chosen to guard the materials. This would make their task much more difficult.

166 *Recounts, supra* note 42 at 5.

167 With more than 1,000 voters in many polling places, the attackers could easily replace enough votes to ensure that Johnny Adams overcame his loss.

168 CAL. ELEC. CODE §19253(b)(2) (2006) provides that the "voter-verified paper audit trail shall govern if there is any difference between it and the electronic record during a one-% manual tally or full recount."

169 *Recounts, supra* note 42 at 5.

170 10 ILL. COMP. STAT. 5/24C-15 (2005).

171 In their 2004 report, *Recommendations of the Brennan Center for Justice & The Leadership Council on Civil Rights for Improving Reliability of Direct Recording Electronic Voting Systems,* (*at* http://www.brennancenter.org/programs/downloads/voting_systems_final_recommendations.pdf), the Brennan Center and the Leadership Conference on Civil Rights recommended that jurisdictions hire independent security experts and create independent security oversight panels to implement and oversee security measures. To the extent that jurisdictions have adopted these proposals, these groups could be present during any forensic investigation to increase its transparency.

172 Where a state determines that electronic records should be given a presumption of authority, the reverse process would be followed: first investigate the electronic records for tampering, then (if necessary) examine the paper records.

173 This number depends upon whether the ballot definition file is created at the vendor or by individual counties. If the vendor creates the ballot definition file for several counties in the state, the Trojan Horse can be inserted into the ballot definition files of multiple counties from a central location. Where each county created its own ballot definition files, at least three informed participants would be necessary (as we have assumed that a successful attack in Pennasota would target a minimum of three counties, three separate individuals with access to each county's ballot definition files would be needed).

174 A full catalog of the attacks against PCOS that have been examined can be found in *Attack Catalogs, supra* note 20.

175 *See supra* notes 88 and 89.

176 *See supra* note 89.

177 The central tabulator is most often employed to perform ballot definition, copying of ballot definition to the memory cards (so that voter choice will be recorded accurately) as well as tabulation of voter choice. The central tabulator is a conventional Personal Computer with additional software added. Accordingly, it provides a convenient single point of attack which one can modify all the print drivers from all the PCOS scanners in a single county.

178 This estimate is based upon a review of 19 contracts executed by counties around the

country for purchase of voting machines. Copies of these contracts are on file at the Brennan Center.

179 *See* Appendix G.

180 7% of 693 votes is 49 votes. If the Software Attack Program targeted 800 machines in the three largest counties, it could switch close to 40,000 votes.

181 *See* Assumptions in Appendix G; this assumes the same make and model PCOS scanner was used throughout the state.

182 This is true with one important caveat: if the PCOS scanners had wireless components, or were in some other way connected to each other or a central location, additional attackers could circumvent Parallel Testing via a remote control command that triggered or superseded the attack.

183 *See supra* pp. 49–50 (Representative "Least Difficult" Attack: Trojan Horse Inserted Into Operating System, DRE Attack Number 4)

184 Specifically, in the 2004 Presidential Election, Central Count Optical Scans had a residual vote rate of 1.7%, compared to just 0.7% for PCOS. In counties with African-American populations of greater than 30%, the residual vote rate for Central Count was 4.1%, and for PCOS just 0.9%. Lawrence Norden, *et al.*, *"Voting System Usability"* in THE MACHINERY OF DEMOCRACY (Brennan Center for Justice ed., forthcoming July 2006).

185 *Id.*

186 N.Y. ELEC. LAW § 7-202 (2006); MINN. STAT. ANN. § 206.845 (2005).

187 Secretary of State for the State of California, *Decertification and Withdrawal of Approval of Certain DRE Voting Systems and Conditional Approval of the Use of Certain DRE Voting System*, at 7 (Apr. 30, 2004) *available at* http://www.ss.ca.gov/elections/ks_dre_papers/decert1.pdf. ("No component of the [DRE] voting system shall include the hardware necessary to permit wireless communications or wireless data transfers to be transmitted or received.")

188 Among them are ES&S and WinVote. *See*, Jay Wrolstad, *Florida Invests $24m in Wireless Voting Machines*, MOBILE TECH TODAY (Jan. 31, 2002) *at* http://www.wirelessnewsfactor.com/perl/story/16104.html; Blake Harris, *A Vote for the Future*, GOVERNMENT TECHNOLOGY MAGAZINE (Aug. 29, 2003) *at* http://www.govtech.net/magazine/story.php?id=61857&issue=8:2003.

189 *See*, Krebs *supra* note 76 ("A previously unknown flaw in Microsoft's Windows operating system is leaving computer users vulnerable to spyware, viruses and other programs that could overtake their machines. . . .").

190 Maryland, which does not require voter-verified paper records, also performs Election Day Parallel Testing. The 12 states that perform must conduct audits of their voter-verified paper records after every election are: AK, CA, CO, CT, HI, IL, MN, NM, NC, NY, WA, and WV.

191 The 26 states are: AK, CA, CO, CT, HI, ID, IL, ME, MI, MN, MO, MT, NC, NH, NJ, NM, NV, NY, OH, OR, SD, UT, VT, WA, WI, and WV.

192 Laws providing for inexpensive candidate-initiated recounts might also add security for voter-verified paper. The Task Force did not examine such recounts as a potential countermeasure.

193 Some DREs and DREs w/VVPT may be designed so that they cannot function unless they are connected to one another. Election officials should discuss this question with voting system vendors.

194 Two other states, West Virginia and Maine, ban networking of machines without banning wireless components themselves. Banning the *use* of wireless components (even when that involves disabling them), rather than requiring *removal* of these components, still leaves voting systems unnecessarily insecure.

[195] *See, Recommendations of the Brennan Center for Justice and the Leadership Conference on Civil Rights for Improving Reliability of Direct Recording Electronic Voting Systems* (2004), http://www.brennancenter.org/programs/downloads/voting_systems_final_recommendations.pdf (recommending that jurisdictions hire independent security experts and create independent security oversight panels to implement and oversee security measures). Independent security experts and oversight panel members should be present during any forensic investigation, to increase its transparency.

[196] When a state determines that electronic records should be given a presumption of authority, the reverse process should be followed: first investigate the electronic records for tampering, then (if necessary) examine the paper records.

[197] As previously discussed, to ensure the robustness of our findings, we ran our analysis against the results of the 2004 presidential race in Florida, New Mexico and Pennsylvania.

[198] Many of these definitions are supplemented by text in the report and Appendices.

[199] *Recounts, supra* note 42 at 3.

[200] For further discussion of inspection and testing performed on voting machines, *see* Appendix E.

[201] NIST's *Glossary of U.S. Voting Systems, at* http://xw2k.sdct.itl.nist.gov/lynne/votingProj/main.asp (Last visited June 10, 2006).

[202] National Security Telecommunications and Information Systems Security Committee, NSA *National Information Systems Security (INFOSEC) Glossary,* NSTISSI No. 4009, at 49 (June 5, 1992), *available at* http://www.cultural.com/web/security/infosec.glossary.html.

[203] For a detailed discussion of a history of fraud against paper-based systems through ballot stuffing, vote buying and other methods, *see* HARRIS, *supra* note 9.

[204] This Appendix is largely borrowed from Douglas Jones's "Testing Voting Machines," part of his *Voting Machines Web Pages,* which can be found at http://www.cs.uiowa.edu/~jones/voting/testing.shtml (Last visited June 10, 2006). We thank Professor Jones for permission to use this material. This material is based upon work partially supported by the National Science Foundation under Grant No. CNS-052431 (ACCURATE). Any opinions, findings or recommendations expressed in this material are those of the author and do not necessarily reflect the views of the National Science Foundation.

[205] The importance of making sure that observer/participant understand how the random numbers are to be used is amusingly illustrated in the magic special: *Penn & Teller: Off the Deep End* (NBC television broadcast, Nov 13th, 2005). In this program an unsuspecting individual is fooled into thinking that the magicians could figure out in advance what card he or she will select because, no matter what card is selected, the magicians can point to its representation somewhere on the beach. The humorous approach here is that all 52 playing cards were set up in interesting ways on the beach to be revealed. A magician opened his coat for one card, two kids in the water held up their rafts to form a card, a sunbather turned around with a card painted on her back, cards were found inside of a potted plant and coconut, *etc.*

[206] Based on the parameters we have set for our election in Pennasota, this would be enough machines to swing the election between Jefferson and Adams. Going back to the assumptions made in this report: the attacker will not want to create a swing of more than 15% on any machine; there are 125 votes recorded per machine; this means the attacker will not want to switch more than 18.75 votes per machine; if her program attacks 2883 machines, she will switch 54,056 votes, more than the 51,891 "target" votes to switch listed in Appendix G.

[207] Again, this assumes that the same make and model DRE is used in the entire state. For suggestions on how to perform Parallel Testing when there are several models of DRE in use in the state, *see* page 88 in this report.

208 Illinois law provides an example of how to make forensic investigations transparent: in the event investigations following a discrepancy revealed in an audit of paper records, the State Board of Elections, State's Attorney or other appropriate law enforcement agencies, the county leader of each established political party in the affected county or counties, and qualified civic organizations be given prior written notice of the time and place and be invited to observe. 10 ILL. COMP. STAT. 5/24C-15

209 Again, Illinois provides an example of one way to increase the transparency of the investigation: the State Board of Elections, State's Attorney or other appropriate law enforcement agencies, the county leader of each established political party in the affected county or counties, and qualified civic organizations are given prior written notice of the time and place of all forensic investigations of machines or paper and are invited to observe.

APPENDIX A
ALTERNATIVE THREAT ANALYSIS MODELS CONSIDERED

Measuring the complexity of the trusted computing base.

Before adopting the threat model discussed in this report, the Task Force considered other potential methods of analysis, including measuring the complexity of the trusted computing base. In computer security terminology, the *trusted computing base* (the "TCB") is the "totality of protection mechanisms within a computing system including hardware, firmware and software, the combination of which is responsible for enforcing a security policy."[202]

For many Task Force members, evaluating the complexity of the TCB was an attractive method for evaluating the relative security of different voting systems. In essence, this methodology would look at how "complicated" the trusted computing base of each system was by reviewing code and other technological complexities. The more complex the TCB, the more likely that it could be attacked without notice.

We quickly realized that this was not a satisfactory way to analyze the relative security of systems. If we only looked at the complexity of the voting system TCB in analyzing its vulnerabilities, we would come to some very strange conclusions and ignore some important historical lessons about election fraud. For instance, under this system of analysis, the hand counting of ballots would carry no risk (there would be no TCB under this system). In fact, as election officials know all too well, pure paper elections have repeatedly shown themselves to be vulnerable to election fraud.[203]

While it may be wise to minimize the total amount of technology we "trust" in elections, as a method for assessing the strength of a voting system and identifying potential weaknesses, it does not appear to provide a useful means of analysis.

Counting points of vulnerability.

A related methodology would be to look at the points of vulnerability within a system. At first blush, this also appeared to be an attractive method for a security analysis. Obviously, we would like to minimize the ways that an attacker might compromise an election. It is easier to guard one door than a thousand.

As a practical matter, however, it did not appear to be a very good way to prioritize threats, or identify vulnerabilities that election officials should be most worried about. Obviously a system with three highly vulnerable points that are impossible to protect is not preferable to a system with four small points of vulnerability that are easy to protect.

Examining Adherence to NIST Risk Assessment Controls.

This model would compare voting systems with guidelines established in NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems. Special Publication 800-30 provides a generic methodology for examining, assessing, and mitigating risk. However, it does not specifically address threats and vulnerabilities unique to the voting environment. For this reason, the Task Force rejected it as a basis for establishing a voting systems threat analysis model.

APPENDIX B
VOTING MACHINE DEFINITIONS

Direct Recording Electronic Voting Machine

A Direct Recording Electronic ("DRE") voting machine directly records the voter's selections in each race or contest. It does so via a ballot that appears on a display screen. Typical DRE machines have flat panel display screens with touch-screen input, although other display technologies have been used (this includes paper and push button displays). The defining characteristic of these machines is that votes are captured and stored electronically.

Software is updated in DRE systems via various methods, specific to each voting system. In general, software updating involves someone (usually a technician or election official representative) installing new software over older software using whatever medium the DRE uses to transport votes (sometimes, it is done using laptop computers, using special software provided by vendors).

Examples of DRE systems include: Hart InterCivic's eSlate, Sequoia's AVC Edge, ES&S's iVotronic, Diebold AccuVote-TS and AccuVote-TSX, AVS WinVote and UniLect Patriot.

Direct Recording Electronic Voting Machine with Voter-Verified Paper Trail

A Direct Recording Electronic Voting Machine with Voter-Verified Paper Trail ("DRE w/VVPT") is a DRE that captures a voter's choice both (1) internally in purely electronic form, and (2) contemporaneously on paper, as a voter-verified record. A DRE w/VVPT allows the voter to view and confirm the accuracy of the paper record.

Examples of DRE w/ VVPT include: AccuPoll, AvanteVote-Tracker EVC-308SPR, Sequoia VeriVote with Printer attachment, TruVote and Diebold Accuview with VVPT Printer attachment.

Precinct Count Optical Scan

Precinct Count Optical Scan ("PCOS") is a voting system that allows voters to mark paper ballots, typically with pencils or pens. Voters then carry their ballots (sleeved or otherwise protected so that others cannot see their choices) by hand to a scanner. At the scanner, they un-sleeve the ballot and insert it into the scanner, which optically records the vote.

Examples of PCOS include: Avante Optical Code Tracker, ES&S Model 100, Sequoia or ES&S Opteck II-P Eagle, Diebold AccuVote-OS.

APPENDIX C
ALTERNATIVE SECURITY METRICS CONSIDERED

Dollars Spent

The decision to use the number of informed participants as the metric for attack level difficulty came after considering several other potential metrics. One of the first metrics we considered was the dollar cost of attacks. This metric makes sense when looking at attacks that seek financial gain – for instance, misappropriating corporate funds. It is not rational to spend $100,000 on the misappropriation of corporate funds if the total value of those funds is $90,000. Ultimately, we rejected this metric as the basis for our analysis because the dollar cost of the attacks we considered were dwarfed by (1) current federal and state budgets, and (2) the amounts currently spent legally in state and federal political campaigns.

Time of Attack

The relative security of safes and other safety measures are often rated in terms of "time to defeat." This was rejected as metric of difficulty because it did not seem relevant to voting systems. Attackers breaking into a house are concerned with the amount of time it might take to complete their robbery because the homeowners or police might show up. With regard to election fraud, many attackers may be willing to start months or years before an election if they believe they can control the outcome. As discussed *supra* pp. 33–47, attackers may be confident that they can circumvent the independent testing authorities and other measures meant to identify attacks so that the amount of time an attack takes becomes less relevant.

APPENDIX D
BRENNAN CENTER SECURITY SURVEY

1. Do you request that your responses remain anonymous?
   ❑ yes ❑ not necessary

2. What type of machine(s) did you use in the last election (please indicate make, model and type)? And do you expect to use different machines within the next two years (if yes, indicate which new machines you expect to use)?

3. Does your jurisdiction provide voters with sample ballots before Election Day?

4. What security measures does your jurisdiction take related to the storage of voting machines?

   a. Are machines stored in a secure location? If so, in what type of location are they stored and how are they made secure?

   b. Are there tamper-evident seals placed on machines? If so, when are they placed around machines? When are they taken off?

   c. Is inventory of machines taken at any time between elections?

   d. Other security measures during storage? If so, please detail these security measures.

5. What security measures does your jurisdiction take when transporting machines to polling place?

   a. How and by whom are the machines transported?

   b. How long between transportation and use on Election Day?

   c. Other security measures during transportation? If so, please detail these security measures.

6. What, if any, testing is done to ensure that the machines are properly recording and tallying votes ("Logic and Accuracy Testing") of machines prior to or on Election Day? If testing is done, please detail who does testing and how it is done.

7. What, if any, security measures do you take on Election Day immediately prior to opening polls?

   a. Inventory of machines, parts (please indicate which parts)?

   b. Check clock on machines?

   c. Check ballots to ensure correct precinct?

   d. Record number of ballots?

   e. Print and sign zero tape?

   f. Other security measures immediately prior to opening polls? If so, please detail these security measures.

8. What, if any, security measures do you take during the period in which polls are open?

   a Entry and exit of each voter to/from polling place recorded in poll books?

   b. If you use DRE with paper trail, is each voter encouraged to verify the accuracy of the paper receipt? If so, how?

   c. If machine is OpScan, is anything done to ensure that overvote protection is not turned off manually? If so, what is done?

   d. If machine is OpScan, is there a stated/written policy for how poll workers should deal with a ballot that is rejected by the machine because of an overvote? If so, what is that policy?

   e. If you use DRE with verified paper trail or OpScans, how is ballot/paper stored after votes have been cast on Election Day?

   f. If there are ballots or machine produced paper, what is done with "spoiled" ballots/paper?

   g. Other security measures taken on Election Day? If so, please detail these security measures.

9. What if any security measures are taken at close of Election Day?

   a. If you have cartridges with ballot images, are these collected to ensure that number of cartridges matches number of machines?

b. Are numbers of blank and spoiled ballots determined?

c. Do poll workers sign ballot tapes? If so, when?

d. How are vote tallies in polling place reported to central office (*e.g.,* phone, modem, other method)?

e. What measures are taken to ensure that polling place vote tallies are accurately recorded at central office?

f. What is done with (i) machine cartridges, (ii) machine tapes, and (iii) poll books at close of election? Are these placed in a secure location? If so, how do you make placement secure (please answer separately for each)?

g. What measures are taken to ensure that valid provisional ballots are accurately counted and secured for potential recounts?

h. If you use OpScan or DRE with a verified paper trail, what is done with these ballots/papers at close of Election Day?

i. Is there any public posting of polling place tallies by individual polling places (other than report to central office)? If so, where is this posting made?

j. What is done with machines at close of the polls, after votes have been counted?

k. Other security measures after close of Election Day? If so, please detail these security measures.

10. The Brennan Center is currently conducting research about voting machines in a variety of areas, including voting machine security. We would very much like to have the insights of election officials, who understand the practical concerns of running an election and ensuring that it is conducted as securely as possible.

We may want to follow up by telephone or e-mail to ask about your responses. Would you have any objection to this?

County, State: _____

Name/Title: _____

Phone/e-mail: _____

Best time to follow up: _____

APPENDIX E
VOTING MACHINE TESTING

An Overview of Voting Machine Testing[204]

Voting systems are subjected to many tests over their lifetimes, beginning with testing done by the manufacturer during development and ending on Election Day. These tests are summarized below, along with a brief description of the strengths and weaknesses of each test.

- Internal testing at the vendor
- Independent Testing Authority certification
- State qualification tests
- Tests conducted during contract negotiation
- Acceptance Testing as delivered
- Pre-election (Logic and Accuracy) testing
- Testing as the polls are opened
- Parallel Testing during an election
- Post-election testing

Internal Testing at the Vendor

All responsible product developers intensively test their products prior to allowing any outsiders to use or test them. The most responsible software development methodologies ask the system developers to develop suites of tests for each software component even before that component is developed. The greatest weakness of these tests is that they are developed by the system developers themselves, so they rarely contain surprises.

Independent Testing Authority Certification

Starting with the 1990 FEC/NASED standards, independent testing authorities (ITAs) have tested voting systems, certifying that these systems meet the letter of the "voluntary" standards set by the federal government and required, by law, in most states. Several states, such as Florida, that impose additional standards contract with the same labs to test to these stronger standards.

The ITA process has two primary weaknesses: First, the standards contain many

specifics that are easy to test objectively (the software must contain no "naked constants" other than zero and one) and others that are vague or subjective (the software must be well-documented). The ITAs are very good at testing to the specific objective requirements, but where subjective judgment or vague requirements are stated, the testing is frequently minimal.

Second, there are many requirements for voting systems that are obvious to observers in retrospect but that are not explicitly written in the standards (*e.g.,* Precinct 216 in Volusia County, Florida reported -16,022 votes for Gore in 2000; prior to this, nobody thought to require that all vote totals be positive). The ITA cannot be expected to anticipate all such omissions from the standards.

Finally, the ITA tests are almost entirely predictable to the developers, as with the vendor's internal testing. Barring outright oversights or carelessness on the part of the vendor, and these do occur, and barring the vendor's decision to use the ITA process in lieu of an extensive internal testing program, the ITA testing can be almost *pro forma*. Catching carelessness on the part of the vendor and offering a guarantee that minimal standards have been met are sufficiently important that the ITA process should not be dismissed out of hand.

State Qualification Tests

While some states allow any voting system to be offered for sale that has been certified to meet the "voluntary" federal standards, many states impose additional requirements. In these states, vendors must demonstrate that they have met these additional standards before offering their machines for sale in that state. Some states contract out to the ITAs to test to these additional standards, some states have their own testing labs, some states hire consultants, and some states have boards of examiners that determine if state requirements are met.

In general, there is no point in having the state qualification tests duplicate the ITA tests. There is considerable virtue in having state tests that are unpredictable, allowing state examiners to use their judgment and knowledge of the shortcomings of the ITA testing to guide their tests. This is facilitated by state laws that give the board members the right to use their judgment instead of being limited to specific objective criteria. Generally, even when judgment calls are permitted, the board cannot reject a machine arbitrarily, but must show that it violates some provision required by state law.

State qualification testing should ideally include a demonstration that the voting machine can be configured for demonstration elections that exercises all of the distinctive features of that state's election law, for example, straight party voting, ballot rotation, correct handling of multi-seat races, and open or closed primaries, as the case may be. Enough ballots should be voted in these elections to verify that the required features are present.

Tests Conducted During Contract Negotiation

When a jurisdiction puts out a request for bids, it will generally allow the finalists to bring in systems for demonstration and testing. It is noteworthy that federal certification and state qualification tests determine whether a machine meets the legal requirements for sale, but they generally do not address any of the economic issues associated with voting system use, so it is at this time that economic issues must be evaluated.

In addition, the purchasing jurisdiction (usually the county) has an opportunity, at this point, to test the myriad practical features that are not legislated or written into any standards. As of 2004, neither the FEC/NASED standards nor the standards of most states address a broad range of issues related to usability, so it is imperative that local jurisdictions aggressively use the system, particularly in obscure modes of use such as those involving handicapped access (many blind voters have reported serious problems with audio ballots, for example).

It is extremely important at this stage to allow the local staff who will administer the election system to participate in demonstrations of the administrative side of the voting system, configuring machines for mock elections characteristic of the jurisdiction, performing pre-election tests, opening and closing the polls, and canvassing procedures. Generally, neither the voting system standards, nor state qualification tests address questions of how easy it is to administer elections on the various competing systems.

Acceptance Testing as Delivered

Each machine delivered by a vendor to the jurisdiction should be tested. Even if the vendor has some kind of quality control guarantees, these are of no value unless the customer detects failures at the time of delivery. At a minimum, such tests should include power-on testing and basic user interface tests (*e.g.,* do all the buttons work, does the touch-screen sense touches at all extremes of its surface, do the paper-feed mechanisms work, does the uninterruptible power supply work).

By necessity, when hundreds or even thousands of machines are being delivered, these tests must be brief, but they should also include checks on the software versions installed (as self-reported), checks to see that electronic records of the serial numbers match the serial numbers affixed to the outside of the machine, and so on.

It is equally important to perform these acceptance tests when machines are upgraded or repaired as it is to perform them when the machines are delivered new, and the tests are equally important after in-house servicing as they are after machines are returned from the vendor's premises.

Finally, when large numbers of machines are involved, it is reasonable to perform more intensive tests on some of them, tests comparable to the tests that ought to be performed during qualification testing or contract negotiation.

Pre-Election (Logic and Accuracy) Testing

Before each election, every voting machine should be subject to public testing. This is frequently described as Logic and Accuracy Testing or simply L&A Testing, a term that is more appropriate in the realm of punch-card and mark-sense ballot tabulating machines than in the realm of direct recording electronic systems, but the term is used widely, and in many states, it is enshrined in state law.

The laws or administrative rules governing this testing vary considerably from state to state. Generally, central-count paper ballot tabulating machinery can be subject to more extensive tests than voting machines, simply because each county needs only a few such machines. Similarly, precinct-count paper ballot tabulating machinery, with one machine per precinct, can be tested more intensively than voting machines, which may number in the tens per precinct.

An effective test should verify all of the conditions tested in Acceptance Testing, since some failures may have occurred since the systems arrived in the warehouse. In addition, the tests should verify that the machines are correctly configured for the specifics of this election, with the correct ballot information loaded, including the names of all applicable candidates, races and contests.

The tabulation system should be tested by recording test votes on each machine, verifying that it is possible to vote for each candidate on the ballot and that these votes are tabulated correctly all the way through to the canvass; this can be done, for example, by casting a different number of votes for each candidate or issue position in each race or contest on the ballot.

When multiple machines are configured identically, this part of the test need only be performed in full and manually on one of the identical machines, while on the others, it is reasonable to simplify the testing by verifying that the other machines are indeed configured identically and then using some combination of automated self-test scripts and simplified manual testing.

For mark-sense voting systems, it is important to test the sensor calibration, verifying that the vote detection threshold is appropriately set between a blank spot on the ballot and a dark pencil mark. The calibration should be tested in terms of pencil marks even in jurisdictions that use black markers because it is inevitable that some voters will use pencils, particularly when markers go dry in voting booths or when ballots are voted by mail. One way to judge the appropriateness of the threshold setting is to see that the system distinguishes between hesitation marks (single dots made by accidentally resting the pencil tip on a voting target) and X or checkmarks, since the former are common accidents not intended as votes, and most state laws allow an X or check to be counted as a vote even though such minimal marks are never recommended.

For touch-screen voting systems, it is important to test the touch-screen calibration, verifying that the machine can sense and track touches over the entire surface of the touch-screen. Typical touch-screen machines have a calibration mode in which they either display targets and ask the tester to touch them with a stylus, or they display a target that follows the point of the stylus as it is slid around the screen.

For voting systems with audio interfaces, this should be checked by casting at least some of the test ballots using this interface. While doing this, the volume control should be adjusted over its full range to verify that it works. Similarly, where multiple display magnifications are supported, at least one test ballot should be voted for each ballot style using each level of magnification. Neither of these tests can be meaningfully performed using automatic self-testing scripts.

The final step of the pre-election test is to clear the voting machinery, setting all vote totals to zero and emptying the physical or electronic ballot boxes, and then sealing the systems prior to their official use for the election.

Ideally, each jurisdiction should design a pre-election test that, between all tested machines, not only casts at least one vote per candidate on each machine, but also produces an overall vote total arranged so that each candidate and each yes-no choice in the entire election receives a different total. Designing the test this way verifies that votes for each candidate are correctly reported as being for that candidate and not switched to other candidates. This will require voting additional test ballots on some of the machines under test.

Pre-election testing should be a public process. This means that the details and rationale of the tests must be disclosed, the testers should make themselves available for questioning prior to and after each testing session, representatives of the parties and campaigns must be invited, and an effort must be made to make space for additional members of the public who may wish to observe. This requires that testing be conducted in facilities that offer both adequate viewing areas and some degree of security.

It is important to assure that the voting machine configuration tested in the pre-election tests is the same configuration used on Election Day. Loading new software or replacing hardware components on a voting machine generally requires the repetition of those parts of the pre-election tests that could possibly depend on the particular hardware or software updates that were made.

Testing as the Polls are Opened

Prior to opening the polls, every voting machine and vote tabulation system should be checked to see that it is still configured for the correct election, including the correct precinct, ballot style, and other applicable details. This is usually determined from a startup report that is displayed or printed when the system is powered up.

In addition, the final step before opening the polls should be to verify that the ballot box (whether physical or virtual) is empty, and that the ballot tabulation system has all zeros. Typically, this is done by printing a zeros report from the machinery. Ideally, this zeros report should be produced by identically the same software and procedures as are used to close the polls, but unfortunately, outside observers without access to the actual software can verify only that the report itself looks like a poll closing report with all vote totals set to zero.

Some elements of the acceptance tests will necessarily be duplicated as the polls are opened, since most computerized voting systems perform some kind of power-on self-test. In some jurisdictions, significant elements of the pre-election test have long been conducted at the polling place.

Observers, both partisan observers and members of the public, must be able to observe all polling place procedures, including the procedures for opening the polls.

Parallel Testing During an Election

Parallel Testing, also known as election-day testing, involves selecting voting machines at random and testing them as realistically as possible during the period that votes are being cast. The fundamental question addressed by such tests arises from the fact that pre-election testing is almost always done using a special test mode in the voting system, and corrupt software could potentially arrange to perform honestly while in test mode while performing dishonestly during a real election.

Parallel Testing is particularly valuable to address some of the security questions that have been raised about Direct Recording Electronic voting machines (for example, touch-screen voting machines), but it is potentially applicable to all electronic vote counting systems.

It is fairly easy to enumerate a long list of conditions that corrupt election software could check in order to distinguish between testing and real elections. It could check the date, for example, misbehaving only on the first Tuesday after the first Monday of November in even numbered years, and it could test the length of time the polls had been open, misbehaving only if the polls were open for at least 6 hours, and it could test the number of ballots cast, misbehaving only if at least 75 were encountered, or it could test the distribution of votes over the candidates, misbehaving only if most of the votes go to a small number of the candidates in the vote-for-one races or only if many voters abstain from most of the races at the tail of the ballot.

Pre-set vote scripts that guarantee at least one vote for each candidate or that guarantee that each candidate receives a different number of votes can be detected by dishonest software. Therefore, Parallel Testing is best done either by using

a random distribution of test votes generated from polling data representative of the electorate, or by asking real voters to volunteer to help test the system (perhaps asking each to flip a coin to decide secretly whether they will vote for the candidates they like or for the candidates they think their neighbor likes).

It is important to avoid the possibility of communicating to the system under test any information that could allow the most corrupt possible software to learn that it is being tested. Ideally, this requires that the particular machines to be tested be selected at the last possible moment and then opened for voting at the normal time for opening the polls and closed at the normal time for closing the polls. In addition, mechanical vote entry should not be used, but real people should vote each test ballot, with at least two observers noting either that the test script is followed exactly or noting the choices made. (A video record of the screen might be helpful.)

Parallel Testing at the polling place is a possibility. This maximizes exposure of the testing to public observation and possibly to public participation, an important consideration because the entire purpose of these tests is to build public confidence in the accuracy of the voting system.

However Parallel Testing is conducted, it is important to guard against any possibility of contamination of the official canvass with ballot data from voting machines that were subject to Parallel Testing. By their very nature, these votes are indistinguishable from real votes, except for the fact that they came from a machine under test. Therefore, physical quarantine of the vote totals from the Parallel Testing is essential. Use of a different color for paper in the printer under test, use of distinctively colored data cartridges, warning streamers attached to cartridges, and similar measures may all be helpful. In addition, if the serial number of the voting machine is tied to its votes through the canvass, a check to make sure that the serial numbers of the machines under Parallel Testing do not appear in the canvass is obviously appropriate.

If polling places are so small that there is no room to select one machine from the machines that were delivered to that polling place, it is possible to conduct Parallel Testing elsewhere, pulling machines for testing immediately prior to delivery to the polling place and setting them aside for testing. In that case, it is appropriate to publish the location of the testing and invite public observation. Casual drop-in observation can be maximized by conducting the tests near a polling place and advertising to the voters at that polling place that they can stop by after voting to watch or perhaps participate.

Post-election Testing

Some jurisdictions require routine post-election testing of some of the voting machinery, to make sure that, after the canvassing process was completed, the machinery is still working as well as it did before the election. Generally, these

tests are very similar to pre-election or Logic and Accuracy Testing.

Clearly, where the machines themselves hold the evidence of the vote count, as with mechanical lever voting machines or direct recording electronic voting machines, this evidence must not be destroyed until law and prudence agree that it is no longer relevant to any potential legal challenge to the election.

In the event of a recount, all of the pre-election tests that do not involve possible destruction of the votes being recounted must be repeated in order to assure that the machinery used in the recount is operating correctly.

APPENDIX F
EXAMPLE OF TRANSPARENT RANDOM SELECTION PROCESSES

A transparent random selection is one where members of the public can verify that, at the time of the choice, all selections were equally probable. Here are two examples of (reasonably) transparent random choice methods. There are many variations on these methods.

Method A: Each member of a group of individuals representing diverse interests chooses a random number (by any method) in a specified range 1...N and writes it down on a slip of paper. After each participant has chosen a number, the numbers are revealed to all and added. They are then divided by N, and the "integer remainder" is the number that is chosen (this is known in mathematics as the "modulo").

The best way to understand this is by example. Little Pennasota County has 9 machines (labeled "1" through "9") and wants to select one of these machines to Parallel Test. They want to ensure that the machine is chosen at random. To do this, they bring together several participants: a member of the League of Women Voters, the Democratic-Republicans, the Federalists, the Green Party, and the Libertarian Party. Each person is asked to select a number. The League of Women Voters' representative selects the number 5, the Democratic-Republican chooses 6, the Federalist chooses 9, the Green chooses 8 and the Libertarian chooses 9. These numbers are then revealed and added: 5+6+9+8+9=37. They are then divided by 9. The integer remainder is 1, because 37 is divisible by 9 four times, with an integer remainder of 1 (or, 36 + 1). In this scenario, machine number 1 is chosen.

Any member of the group can assure the result is not "fixed" by the others. In the example above, all of the political parties might want to conspire to ensure that machine number 2 is picked for Parallel Testing. However, the League of Women Voters representative will prevent them from being able to do this: without knowing what number she is going to pick, they cannot know what the integer remainder will be.

Method B: Color-coded, transparent 10-sided dice are rolled (in a dice cup) in public view. The digits on the top faces of the dice are read off in a fixed order determined by the colors (*e.g.*, first red, then white, then blue). This yields a random 3-digit number. If the number is out of the desired range, it is discarded and the method performed again.

Note about transparently random selection process:

For a transparently random selection process to work, (1) how the randomly selected number is going to be used must be clearly stated in advance (*i.e.*, if we

are choosing a number to decide which machine to parallel test, each machine must be labeled with one of the numbers that may be chosen), (2) the process for randomly selecting numbers must be understood by all participants, and (3) the event of randomly selecting numbers must be observable to all participants (and, if possible, members of the public).

For example, if we are picking what team of police are going to be left to look after the locked-up and security-sealed election materials before completion of the Automatic Routine Audit, the observers and participants must see the committed list of police that are being selected from in advance of the selection. The list must be posted visibly or in some other way "committed to" so that the association between random numbers selected and people selected cannot be switched after the numbers are produced.

In terms of assigning auditors to roles and machines to be audited, the goal might be to make sure that there is one Democratic-Republican and one Federalist assigned to review the paper records (the readers) and one Democratic-Republican and one Federalist assigned to tally the records (the writers). There should be no way to know what machines anyone will be assigned to, nor who will be teamed with whom during the audit.

If the use or interpretation of the random numbers is not clear and committed in advance, then an appropriately situated attacker might "interpret" the random number in a way that allows the attack go undetected by, for example, assigning attackers as auditors for all the subverted machines.[205]

APPENDIX G
ASSUMPTIONS

FACTS/ ASSUMPTIONS ABOUT THE PENNASOTA GOVERNOR'S RACE REFERRED TO IN THIS REPORT

GENERAL FACTS/ASSUMPTIONS ABOUT PENNASOTA IN 2007

Total Number of votes cast in gubernatorial election	3,459,379
Votes Cast for Tom Jefferson	1,769,818
Votes Cast for Johnny Adams	1,689,561
Margin of victory (votes) for Tom Jefferson	80,257
Margin of victory (%) for Tom Jefferson	2.32%
Target % votes to change in favor of Adams	3.0%
Target votes to add or subtract in hypothetical attacked election	103,781
Target votes to switch in Governor's Race	51,891

LIMITS ON ATTACKER

Maximum % of Votes Added or Subtracted Per County:	10% (5% switch)
Maximum % of Votes Added or Subtracted Per Polling Place:	15%(7.5% switch)
Maximum % of Votes Added or Subtracted Per Voting Machine	30% (15% switch)

FACTS/ASSUMPTIONS ACROSS SYSTEMS

Minimum Number counties attacked	3
Total Number of polling places in State	3,030
Number of votes per polling place	1,142
Number polling stations that must be attacked where less than 15% of votes are added or subtracted	606
Minimum Number of Attackers to develop and install Trojan Horse	1
Minimum Number of Attackers to parameterize Trojan Horse	1
Number of machines unusable per polling place to create "bottleneck"	3
Maximum number of discouraged voters (decide not to vote) per polling place under bottleneck	88 (7.7%)
Number of votes potentially gained at polling place under bottleneck	70
Maximum % of unfriendly voters in targeted polling places under bottleneck	90%
Percentage of friendly – foe votes under bottleneck	10%

Number of observers of polling book	1
Number of people needed to delete voters from poll book per polling place	1
Number of people required to modify enough poll books to change outcome of statewide election	606
Number of times single person can fraudulently vote	10
Number of people required to subvert audit	386

GENERAL ASSUMPTIONS FOR THREE LARGEST COUNTIES IN PENNASOTA: MEGA, CAPITAL AND SUBURBIA

Number of polling places in 3 largest counties	1,133
Number of precincts/Election Districts in 3 largest counties	1,669
Number of votes in 3 largest counties	1,156,035
Number of votes stored at largest tally center	531,584
Number of votes stored at the second largest tally center	360,541
Number of votes stored at third largest tally center	263,936
% of votes that would need to be switched in the 3 largest counties to change outcome of governor's race	4.49%

VVPT-RELATED ASSUMPTIONS

Number of votes per DRE w/VVPT	120
Number DREs w/VVPT in state	28,828
Number DREs w/VVPT in 3 largest counties	9634
Number of VVPT that must be changed to win election (assuming no more than 30% of votes switched on any roll)	2,934
Number of people required to create fake VVPT printouts to be replaced after polls close	3

PCOS AND BMD-RELATED ASSUMPTIONS

Total number of PCOS machines in state	4,820
Total number of votes per PCOS machine	606
Total number of PCOS machines in 3 largest counties	1,669
Number of people required to replace ballots with counterfeits per polling place	1
Number of people required to replace sufficient ballots with counterfeit complete ballots	606
Number of people required to steal or counterfeit ballot paper	5

DRE-RELATED ASSUMPTIONS

Number DREs in state	27,675
Number DREs in 3 largest counties	9,248
Number of votes per DRE machine	125
Number of machines under Parallel Testing	58
Number of people required to subvert Parallel Testing	58
Maximum number of votes switched on DRE	18.75
Minimum number of DREs attacked to swing election	2817

AUDIT ASSUMPTIONS

Number of votes audit team can audit in one day	120
Number of auditors per team	2
Number of votes audited in 3 largest counties (2% audit)	23,121
Number of audit teams to conduct audit in 3 largest counties in one day	193
Total number of auditors in 3 largest counties	386

APPENDIX H

TABLES SUPPORTING PENNASOTA ASSUMPTIONS

PENNASOTA COMPOSITE FROM VOTES IN THE 2004 BATTLEGROUND STATES
(TAKEN FROM ACTUAL 2004 PRESIDENTIAL VOTE)

State	Total Votes for Adams (Kerry)	Total Votes for Jefferson (Bush)	Largest Three Counties in State by Population (in descending order)	Number of Votes for Adams (Kerry) by County	Number of Votes for Jefferson (Bush) by County
Colorado	1,001,725	1,101,256	Denver	166,135	69,903
			El Paso	77,648	161,361
			Jefferson	126,558	140,644
Florida	3,583,544	3,964,522	Miami-Dade	409,732	361,095
			Broward	453,873	244,674
			Palm Beach	328,687	212,688
Iowa	741,898	751,957	Polk	105,218	95,828
			Linn	60,442	49,442
			Scott	42,122	39,958
Michigan	2,279,183	2,313,746	Wayne	600,047	257,750
			Oakland	319,387	316,633
			Macomb	196,160	202,166
Minnesota	1,445,014	1,346,695	Hennepin	383,841	255,133
			Ramsey	171,846	97,096
			Dakota	104,635	108,959
Nevada	397,190	418,690	Clark	281,767	255,337
			Washoe	74,841	81,545
			Carson	9,441	13,171
New Mexico	370,942	376,930	Bernalillo	132,252	121,454
			Dona Ana	31,762	29,548
			Santa Fe	47,074	18,466
Ohio	2,741,165	2,859,764	Cuyahoga	448,503	221,600
			Franklin	285,801	237,253
			Hamilton	199,679	222,616

Pennsylvania	2,938,095	2,793,847	Philadelphia	542,205	130,099
			Allegheny	368,912	271,925
			Montgomery	222,048	175,741
Wisconsin	1,489,504	1,478,120	Milwaulkee	297,653	180,287
			Dane	181,052	90,369
			Waukesha	73,626	154,926
Total Votes Per Candidate (2.32% margin of victory)	1,769,818	1,689,561	Average Votes of Three Largest Counties	674,295	481,767
Average Total Votes Per Candidate	3,439,379				

SOURCES: 2004 PRESIDENTIAL ELECTION VOTE TOTALS

Colorado
County: http://www.census.gov/popest/counties/tables/CO-EST2004-01-08.xls
Elections: http://www.elections.colorado.gov/WWW/default/Prior%20Years%20Election%20Information/2004/Abstract%202003%202004%20082305%20Late%20PM-5.pdf
Florida
County: http://www.stateofflorida.com/Portal/DesktopDefault.aspx?tabid=95#27103
Elections: http://election.dos.state.fl.us/elections/resultsarchive/Index.asp?ElectionDate=11/2/04&DATAMODE=
http://www.cnn.com/ELECTION/2004//pages/results/states/FL/P/00/county.000.html
Idaho
http://www.census.gov/popest/counties/tables/CO-EST2004-01-16.xls
http://www.idsos.state.id.us/ELECT/RESULTS/2004/general/tot_stwd.htm
http://www.idsos.state.id.us/ELECT/RESULTS/2004/general/cnty_pres.htm
Michigan
http://www.census.gov/popest/counties/tables/CO-EST2004-01-26.xls
http://miboecfr.nicusa.com/election/results/04GEN/01000000.html
Minnesota
http://www.census.gov/popest/counties/tables/CO-EST2004-01-27.xls
http://electionresults.sos.state.mn.us/20041102/
Wisconsin
http://www.census.gov/popest/counties/tables/CO-EST2004-01-55.xls
http://165.189.88.185/docview.asp?docid=1416&locid=47
Pennsylvania
http://www.census.gov/popest/counties/tables/CO-EST2004-01-42.xls
http://www.electionreturns.state.pa.us/ElectionReturns.aspx?Control=StatewideReturnsByCounty&ElecID=1&OfficeID=1#P
Ohio
http://www.census.gov/popest/counties/tables/CO-EST2004-01-39.xls
http://www.sos.state.oh.us/sos/ElectionsVoter/results2004.aspx?Section=135
Nevada
http://www.census.gov/popest/counties/tables/CO-EST2004-01-32.xls
http://www.cnn.com/ELECTION/2004/pages/results/states/NV/P/00/county.000.html
New Mexico
http://www.census.gov/popest/counties/tables/CO-EST2004-01-35.xls
http://www.cnn.com/ELECTION/2004/pages/results/states/NM/P/00/county.000.html

AVERAGE VOTES FOR THE THREE LARGEST COUNTIES IN THE 2004 BATTLEGROUND STATES

Composite Counties	Adams (Kerry)	Jefferson (Bush)
Mega County	336,735	194,849
Capital County	202,556	157,985
Suburban County	135,003	128,934
Total of Averages	674,295	481,767

PENNASOTA COMPOSITE OF POLLING PLACES AND PRECINCTS IN THE 2004 BATTLEGROUND STATES

State	County	Number of Polling Places (Nov 2004 elections unles otherwise indicated)	Number of Precincts November 2004	Number of Polling Places Statewide	Number of Precincts Statewide
Colorado	Denver	288	422	2,318	3,370
	El Paso	185	378		
	Jefferson	323	330		
Florida	Miami-Dade	534	749	5,433	6,892
	Broward	520	777		
	Palm Beach	420	692		
Iowa	Polk	180	183	1,916	1,966
	Linn	85	86		
	Scott	63	63		
Michigan	Wayne	670	1,198	3,890	5,235
	Oakland	432	549		
	Macomb	259	383		
Minnesota	Hennepin	431*	430	3,750**	4,108
	Ramsey	178	178		
	Dakota	137	137		
New Mexico	Bernalillo	162****	413****	612	684
	Dona Ana	78	108		
	Santa Fe	50	86		
Nevada	Clark	329	1,042	526	1,585
	Washoe	118	250		
	Carson	2	26		

Ohio	Cuyahoga	584	1,436	6,602	11,366
	Franklin	514	788		
	Hamilton	593	1,013		
Pennsylvania	Philadelphia	1,637	1,681	4,000	9,432
	Allegheny	1,214	1,214		
	Montgomery	407	407		
Wisconsin	Milwaukee	N/A ***	N/A***	1,253	3,563
	Dane				
	Waukesha				
Statewide Average of 10 States				2,969	4,820

SOURCE

Unless otherwise indicated, information is from the data tables at the EAC *2004 Election Day Survey, available at* http://www.eac.gov/election_survey_2004/state_data.htm.

* 341 as of June 29, 2005. Telephone interview with Hennepin County Elections Board representative (November 7, 2005).

** Figure is estimated. Telephone interview with Minnesota Secretary of State representative (February 21, 2005).

***Number of Precincts and Polling Places N/A because elections are administered at municipality level and data were not centralized at county level. Milwaukee City, the largest municipality in Milwaukee County, has 202 polling places. Telephone interview with Milwaukee County Election Commission representative (November 7, 2005).

****Telephone interview with Bernalillo County Clerk's Office representative (November 14, 2005).

AVERAGE NUMBER OF PRECINCTS AND POLLING PLACES FOR THE THREE LARGEST COUNTIES IN THE 2004 BATTLEGROUND STATES

Composite Counties	Precincts	Polling Places
Mega County	502	839
Capital County	347	481
Suburban County	250	349
Total of Averages	1,099	1,669

APPENDIX I
DENIAL-OF-SERVICE ATTACKS

December 7, 2005
From: Professor Henry Brady, University of California, Berkeley
To: The Task Force

Denial of the Vote: You asked what the typical distribution of spreads was in precincts. I've gone to two data sets that were readily at hand – Broward and Palm Beach County Florida for the 2000 Presidential race. These are both heavily democratic counties. Roughly Broward was 67% for Gore and Palm Beach was 60% for Gore.

Here are the frequencies by precinct "binned" into 10 intervals from 0% to 100% voting for Gore:

GOREPCC1—BROWARD COUNTY FLORIDA, 2000 PRESIDENTIAL — % GORE VOTE

	Bin Number	% Voting for Gore	Frequency	% of Precincts	Valid %	Cumulative %
Valid	1.00	0-10%	13	1.7	1.7	1.7
	2.00	10-20%	2	.3	.3	2.0
	3.00	20-30%	3	.4	.4	2.4
	4.00	30-40%	15	1.9	2.0	4.4
	5.00	40-50%	73	9.3	9.8	14.2
	6.00	50-60%	132	16.8	17.7	31.9
	7.00	60-70%	217	27.6	29.0	60.9
	8.00	70-80%	124	15.8	16.6	77.5
	9.00	80-90%	87	11.1	11.6	89.2
	10.00	90-100%	81	10.3	10.8	100.0
Total			747	95.2	100.0	
Missing System			38	4.8		
Total			785	100.0		

GOREPCCT—PALM BEACH COUNTY FLORIDA — 2000 PRESIDENTIAL—% GORE VOTE

	Bin Number	% Voting for Gore	Frequency	% of Precincts	Valid %	Cumulative %
Valid	1.00	0-10%	7	1.1	1.1	1.1
	2.00	10-20%	8	1.3	1.3	2.4
	3.00	20-30%	5	.8	.8	3.3
	4.00	30-40%	42	6.7	6.8	10.1

	5.00	40-50%	123	19.6	20.0	30.1
	6.00	50-60%	150	23.9	24.4	54.5
	7.00	60-70%	123	19.6	20.0	74.5
	8.00	70-80%	64	10.2	10.4	84.9
	9.00	80-90%	52	8.3	8.5	93.3
	10.00	90-100%	41	6.5	6.7	100.0
Total			615	98.1	100.0	
Missing System			12	1.9		
Total			627	100.0		

Note that there are lots of precincts with 90% or higher Gore vote (10% in Broward and 6.5% in Palm Beach). These precincts are rather large (730 ballots cast on average in Broward and 695 ballots cast in Palm Beach).

Here are the Bush results for Palm Beach.

BUSHPCCT—PALM BEACH COUNTY FLORIDA 2000 PRESIDENTIAL % BUSH VOTE

	Bin Number	% Voting for Gore	Frequency	% of Precincts	Valid %	Cumulative %
Valid	1.00	0-10%	55	8.8	8.9	8.9
	2.00	10-20%	49	7.8	8.0	16.9
	3.00	20-30%	76	12.1	12.4	29.3
	4.00	30-40%	148	23.6	24.1	53.3
	5.00	40-50%	157	25.0	25.5	78.9
	6.00	50-60%	87	13.9	14.1	93.0
	7.00	60-70%	27	4.3	4.4	97.4
	8.00	70-80%	3	.5	.5	97.9
	9.00	80-90%	6	1.0	1.0	98.9
	10.00	90-100%	7	1.1	1.1	100.0
Total			615	98.1	100.0	
Missing System			12	1.9		
Total			627	100.0		

Note that there are a lot fewer precincts with high Bush vote – only about 2.1% with 80% or greater Bush vote. But, of course, Palm Beach was a very highly Democratic County. Here are the results for Broward:

BUSHPCC1—BROWARD COUNTY FLORIDA — 2000 PRESIDENTIAL — BUSH VOTE

	Bin Number	% Voting for Gore	Frequency	% of Precincts	Valid %	Cumulative %
Valid	1.00	0-10%	94	12.0	12.6	12.6
	2.00	10-20%	96	12.2	12.9	25.4
	3.00	20-30%	144	18.3	19.3	44.7
	4.00	30-40%	211	26.9	28.2	73.0
	5.00	40-50%	122	15.5	16.3	89.3
	6.00	50-60%	53	6.8	7.1	96.4
	7.00	60-70%	11	1.4	1.5	97.9
	8.00	70-80%	1	.1	.1	98.0
	9.00	80-90%	2	.3	.3	98.3
	10.00	90-100%	13	1.7	1.7	100.0
Total			747	95.2	100.0	
Missing System			38	4.8		
Total			785	100.0		

Note that we have about the same situation for Broward.

This suggests that it would be harder to do a "denial of the vote" for Bush than for Gore in these counties. But, of course, in a Presidential race you would probably first choose a county that was heavily in the direction of the other party – hence, if you were a Republican you would choose Palm Beach or Broward Counties and you would not choose heavily Republican counties in the North of Florida.

These tables are typical of what we see around the country.

APPENDIX J

CHANCES OF CATCHING ATTACK PROGRAM THROUGH PARALLEL TESTING

The Automatic Routine Audit and Parallel Testing should both use random sampling of precincts or voting machines to try to catch misbehavior. The attacker doesn't know ahead of time which precincts or machines will be checked and, if there are enough random samples taken, she cannot tamper with a substantial number of precincts or machines without a big risk of her tampering being caught. The question we address in this Appendix is how many machines must be randomly tested to reliably detect a certain level of tampering.

One way to visualize the way random sampling can work is to imagine a room full of ping pong balls. Most of the balls are blue, but a small fraction (say, 1/2 of 1%) are red. When we sample them, we reach into the bin without looking and draw out a ball; we want to know whether we are likely to draw out a red ball in a certain number of tries.

We can imagine a literal version of this, with each ball or slip of paper having a different machine or polling place ID on it. In the case of Parallel Testing, we select machines by drawing these balls out of the bin and sampling only what is indicated by those balls. If we draw a ball representing a machine whose results have been tampered with, we will detect the tampering; if none of the tampered machines is tested, the attacker will get away with her tampering. This idea is very general – it can be applied to Automatic Routine Audits of polling places, precincts or voting machines, Parallel Testing of machines, careful physical inspection of tamper-evident seals on ballot boxes, inspection of polling places for compliance with election laws, *etc.*

The way we really do this is called "sampling without replacement," which just means that when we draw a ball out of the bin, we don't put it back. The probablities of finding the red ball changes each time we draw a ball out. If we have a reasonably large number of balls in the bin and if we are sampling a small percentage, we can use a much simpler formula for sampling with replacement that's approximately correct. This binomial estimate will generally err in a conservative direction, *i.e.,* we will draw a sample larger than necessary.

It's easy to convince yourself that drawing more balls from this bin makes you more likely to get one of the rare balls. It is also easy to see that the more red balls there are in the bin, the more likely you are to draw one out.

We can write formulas to describe all this more precisely. Suppose that in Pennasota there are 28,828 DREs, and 2,883 (or 10%) have been tampered with.[206] We're going to test 10 machines. We want to know how likely we are to detect the tampering.

The easiest way to think of this is to ask how likely we are to fail to detect the tampering. (If we have a 10% chance of failing to detect the tampering, that's just another way of saying we have a 90% chance of detecting it.) Each time we draw a ball from the bin, we have approximately a (2,883/28,828) = 0.10 chance of getting a ball that represents one of the tampered machines. The probability that we'll fail to sample a tampered machine each time is approximately 0.90. To figure out what the probability is that we will fail to sample one of the tampered ones 10 times in a row, we just multiply the probabilities together: 0.90 * 0.90 * ... * 0.90 = $(0.90)^{10}$ = 0.35. So, after 10 samples, we have about a 35% chance of not having caught the attacker. Another way of saying the same thing is that we have about a 100% – 35% = 65% chance of catching the attacker.

An approximate formula for this is:

C = fraction compromised
N = number sampled

$$\text{Probability[detect attack]} = 1 - (1 - C)^s$$

Writing the probabilities as percentages, this looks like:

$$\text{Probability[detect attack]} = 100\% - (100\% - C)^s$$

Now, the question we really care about is how many samples we must take to have some high probability of detecting an attack. That is, we may start knowing the P[detect attack] value we want and need to work backward to find how many samples we must take if the attacker has tampered with 10% of our machines. The general (approximate) formula is

D = probability of detection
C = fraction compromised
N = number sampled

$$N = \log(1 - D) / \log(1 - C)$$

where log() is just the logarithm of these probabilities. The base of the logarithm doesn't matter.

Some sample values for this, with D = 95%. (That is, we require a 95% chance of catching the tampering.)

% Compromised	Number Sampled
0.5%	598
1.0%	298
2.0%	148
5.0%	58
10.0%	28
25.0%	10

This formula and table are approximate. For small numbers of machines or precincts being sampled, they overstate the number of samples needed to get the desired probability, which means that following them may lead you to be a little more secure than you need to be.

So even if we assume that only 5% of machines are tampered with, Parallel Testing of 58 machines should give us a 95% chance of catching a machine that has been tampered with.[207]

APPENDIX K

CHANCES OF CATCHING ATTACK PROGRAM THROUGH THE ARA

From the math already done in Appendix J, we can create this formula:

As already discussed, the formulas listed in Appendix J will apply just as well when attempting to determine whether a 2% audit will have a good chance of catching a fraud.

There are more than 28,000 DREs w/VVPT in Pennasota, with an average of 120 voters per machine. As our attacker wants to avoid detection, we have assumed that she will create an attack program that will switch a limited number of votes in each polling place – specifically about 18 (or 15% of all votes) per machine. Assuming she wants to switch about 52,000 votes, this comes out to an attack on about 1600 machines.

What is the probability of catching this fraud with a 2% audit? In a 2% audit, we will audit about 560 machines.

The fraction of bad machines is 1,600/28,000 or 0.055.

Each time we audit a machine, we have a chance of 0.055 of picking a machine that has been tampered with, and a chance of 1 – 0.055 (or 0.945) of picking a machine that has not been tampered with.

The probability of picking *only* machines that have not been tampered with after auditing all 560 machines is $(1 - C)^s$ or $(0.945)^{560}$. This is extremely close to zero, which means that the chances of *not* catching the fraud are less than 1%; conversely, the chances of catching it are close to 100%.

Paper replaced

But what if the attacker had pollworkers in 550 polling places replace the paper before it reached county headquarters for the ARA? This would leave, at a minimum 56 rolls that are evidence of the fraud (assuming that in the 56 polling places where paper wasn't replaced, there was only one DRE per polling site). This means roughly 0.2% of paper rolls would show that the paper did not match the electronic records. What are the chances that a 2% audit (or audit of 560 machines) would catch this?

This time, each time we audit the paper rolls, the chances of catching a paper roll with evidence of the fraud is 56/28,000, or roughly 0.002. So the probability of picking *only* rolls that do not show evidence of fraud after auditing all 560 rolls and machines is $(.998)^{560}$, or about 1/3. Thus, there would still be a 2/3 chance that the fraud would be detected.

APPENDIX L
SUBVERTING THE AUDIT

Parallel Testing

We've described auditing processes that can detect all kinds of misbehavior. However, this leaves open a question: How many auditors must our attacker corrupt to prevent the detection of misbehavior?

Preliminaries
We assume that auditing or Parallel Testing is done by teams. Each team is somehow put together from one or more auditors, and each team is assigned randomly to a subset of the things being audited.

How Many Corrupt Auditors Subvert an Audit Team?
How many corrupt auditors does it take to subvert an audit team? The answer depends on the procedures used for auditing. The two extreme cases are of the greatest interest:

- One Bad Apple: As discussed on page 55 of this report, during Parallel Testing, it is likely that a single corrupt auditor can enter a Cryptic Knock that will inform a tampered machine that it is being Parallel Tested. If the tester cannot enter a Cryptic Knock (because this feature was not part of the attack program) then all members of the Parallel Testing team will have to be subverted.

- The Whole Bunch: During hand-recounts of paper ballots, reasonable procedures can make it very difficult for an audit team with even one uncorrupted auditor to fail to detect any significant fraud (that is, more than two or three votes).

We will consider these two models below.

Impact of Corrupted Audit Teams
The best way to think about the impact of a corrupt audit team is to omit the audits done by that team from the total number of audits we assume are done. Thus, if we have ten teams, each doing 5 audits, and we assume two teams are corrupt, then instead of calculating the probability of detecting an attack based on 50 audits being done, we calculate it based on the probability of 40 audits being done.

Some Simple Approximations
Here is a simple, conservative approximation of the expected value and 95% upper limit on the number of compromised audit teams. We compute the probability that a team will get corrupted, and then use binomial distribution to determine the expected number of corruptions. We assume sampling without replace-

ment for teams based on a fixed proportion of corrupt auditors. This is also over-simplified and conservative, but less so than the super-simple model.

Let:

R be the total number of auditors, of whom N are corrupt.
The proportion of corrupt auditors is N/R
Each team consist of K auditors
$Q = R/K$ = the total number of teams

For the one corrupt auditor model:
(That is, a single corrupt auditor subverts the whole team.)

The probability of a team being corrupted is $P = 1 - ((R - N) / R)^K$.
This is 1 minus the probability that all the auditors on a team are not corrupt.

For the all corrupt model:
(That is, all the auditors on the team must be corrupt to corrupt the team.)

The probability of a team being corrupted is $P = (N/R)^K$.

For both models:

Prob(M corrupted audit teams) = Choose(Q,M) $P^M (1 - P)^{(Q-M)}$
Expected number of corrupted audit teams = $P*Q$
S = standard deviation = Sqrt($P*(1 - P)*Q$)
95% upper bound on corrupted audit teams = $P*Q + 1.64*S$

The biggest thing to notice about these formulas is that when you need to corrupt all members of a team to corrupt the team, you need to corrupt practically all the auditors to have much of an impact. For example, consider an election with 100 auditors, 5 to a team. Here are some numbers when we have to have all auditors on a team corrupted to subvert that team's audits: (There are 20 teams total.)

Corrupt Auditors	Corrupt Teams Expected	95% Upper Bound
10	0	0
20	0	0
30	0	0
40	0	1
50	1	2
60	2	4
70	3	6
80	7	10
90	12	15

The 95% upper limit here means the true number of corrupt teams should not exceed the upper limit in 95% of the possible teams drawn. The critical value of 1.64 is based on the commonly used normal distribution. *Note the implications for parameters of our audit teams – bigger teams are much better than smaller

ones. If we had audit teams of one, corrupting half the auditors would corrupt half the audits, while here it corrupts only 10% of the audits. On the other hand, we could do five times as many audits with one auditor to a team.

On the other hand, the attacker has a much easier time attacking auditing processes where a single corrupted participant subverts the whole audit process. Similar numbers then look like:

Corrupt Auditors	Corrupt Teams Expected	95% Upper Bound
10	8	11
20	13	16
30	17	19
40	18	20
50	19	20
60	20	20
70	20	20

In this case, small audit/Parallel Testing teams make more sense.

Bribing The Audit Teams in Pennasota to Subvert the Audit

If our attacker could successfully bribe auditors to "cheat" during the audit, so that they would ignore discrepancies between the paper and electronic records, how many would he have to bribe? Our analysis shows that nearly all of the auditors in the largest counties would have to be successfully bribed if the attack was to work.

We can use the audit in Pennasota's three largest counties, Mega, Capitol and Suburbia, as an example. With a 2% audit, 193 teams of two will audit one DRE w/VVPT paper roll each (each paper roll will contain approximately 120 votes). Each member of each team of auditors is selected by one of the major political parties; after they are selected and immediately before the auditing begins, they are randomly assigned a partner and a machine. Every team has one Federalist and one Democratic-Republican.

What fraction of these auditors must the attackers corrupt to avoid her attack being caught? If τ represents the fraction of auditors from each party that our attacker must corrupt, and each party's auditor is randomly matched with an auditor from the other party, the probability of an entire audit team being corrupted (i.e. both auditors being corrupted) is τ^2.

A machine passes an audit if:

(1) it is a good machine; or

(2) it is a bad machine but both auditors are corrupted.

The probability of (1) is $1 - C$. The probability of (2) is $C\tau^2$ Thus the probability of a machine passing the audit is

$$1 + C(\tau^2 - 1).$$

And the probability of S machine passing the audit is approximately:

$$\rho = (1 + C(\tau^2 - 1))^S$$

Solving this equation for τ yields:

$$\tau = \sqrt{\frac{\rho^{(1/S)} - 1}{C} + 1}$$

We have assumed that the attacker would need to attack 1,602 DREs w/VVPT to feel comfortable that he could change the outcome of the governor's race in Pennasota. There are 9,634 DREs w/VVPT in Pennasota's three largest counties. Thus, C=1602/9634 or 0.17. S, the number of machines and paper rolls audited is 193. Assuming that our attacker wants 90% certainty that she will subvert the audit, ρ equals 0.9.

Accordingly, the percentage of auditors that must be successfully bribed to subvert the audit is close to approximately 99.7%.

APPENDIX M

EFFECTIVE PROCEDURES FOR DEALING WITH EVIDENCE OF FRAUD OR ERROR

The following are examples of procedures that would allow jurisdictions to respond effectively to detection of bugs or Software Attack Programs:

1. Impound and conduct a transparent forensic examination[208] of all machines showing unexplained discrepancies during Parallel Testing;

2. Where evidence of a software bug or attack program is subsequently found (or no credible explanation for the discrepancy is discovered), conduct a forensic examination of all DREs in the state used during the election;

3. Identify the machines that show evidence of tampering or a software flaw that could have affected the electronic tally of votes;

4. Review the reported margin of victory in each potentially affected race;

5. Based upon the (a) margin of victory, (b) number of machines affected, and (c) nature and scope of the tampering or flaw, determine whether there is a substantial likelihood that the tampering or flaw changed the outcome of a particular race; and

6. Where there is a substantial likelihood that tampering changed the outcome of a particular race, hold a new election for the office.

The following are examples of procedures that would allow jurisdictions to respond effectively to detection of statistical anomalies in the voter-verified paper record:

1. Conduct a transparent forensic investigation of machines[209] that have produced paper records with significant statistical anomalies;

2. To the extent tampering with any of these machines is found, conduct a similar investigation of all machines in the State;

3. After quantifying the number of machines that have been tampered with, determine the margin of victory in each potentially affected race;

4. Based upon the (a) margin of victory, (b) number of machines affected, and (c) nature and scope of the tampering, determine whether there is a substantial likelihood that tampering changed the outcome of a particular race; and

5. In the event that a determination is made that there is a substantial likelihood that tampering changed the outcome of a particular race, hold a new election for the office.

BRENNAN CENTER FOR JUSTICE
BOARD OF DIRECTORS AND OFFICERS

James E. Johnson, Chair
Partner,
Debevoise & Plimpton LLP

Michael Waldman
Executive Director,
Brennan Center for Justice

Nancy Brennan
Executive Director,
Rose Kennedy
Greenway Conservancy

Zachary W. Carter
Partner, Dorsey & Whitney LLP

John Ferejohn
Professor, NYU School of Law
& Stanford University

Peter M. Fishbein
Special Counsel, Kaye Scholer

Susan Sachs Goldman

Helen Hershkoff
Professor, NYU School of Law

Thomas M. Jorde
Professor Emeritus, Boalt Hall
School of Law – UC Berkeley

Jeffrey B. Kindler
Vice Chairman & General Counsel,
Pfizer Inc.

Ruth Lazarus

Nancy Morawetz
Professor, NYU School of Law

Burt Neuborne
Legal Director, Brennan Center
Professor, NYU School of Law

Lawrence B. Pedowitz
Partner,
Wachtell, Lipton, Rosen & Katz

Steven A. Reiss,
General Counsel
Partner, Weil, Gotshal
& Manges LLP

Richard Revesz
Dean, NYU School of Law

Daniel A. Rezneck
Senior Trial Counsel, Office of the
DC Corporation Counsel

Cristina Rodriguez
Assistant Professor, NYU School
of Law

Stephen Schulhofer
Professor, NYU School of Law

John Sexton
President, New York University

Sung-Hee Suh
Partner,
Schulte Roth & Zabel LLP

Robert Shrum
Senior Fellow,
New York University

Rev. Walter J. Smith, S.J.
President & CEO,
The Healthcare Chaplaincy

Clyde A. Szuch

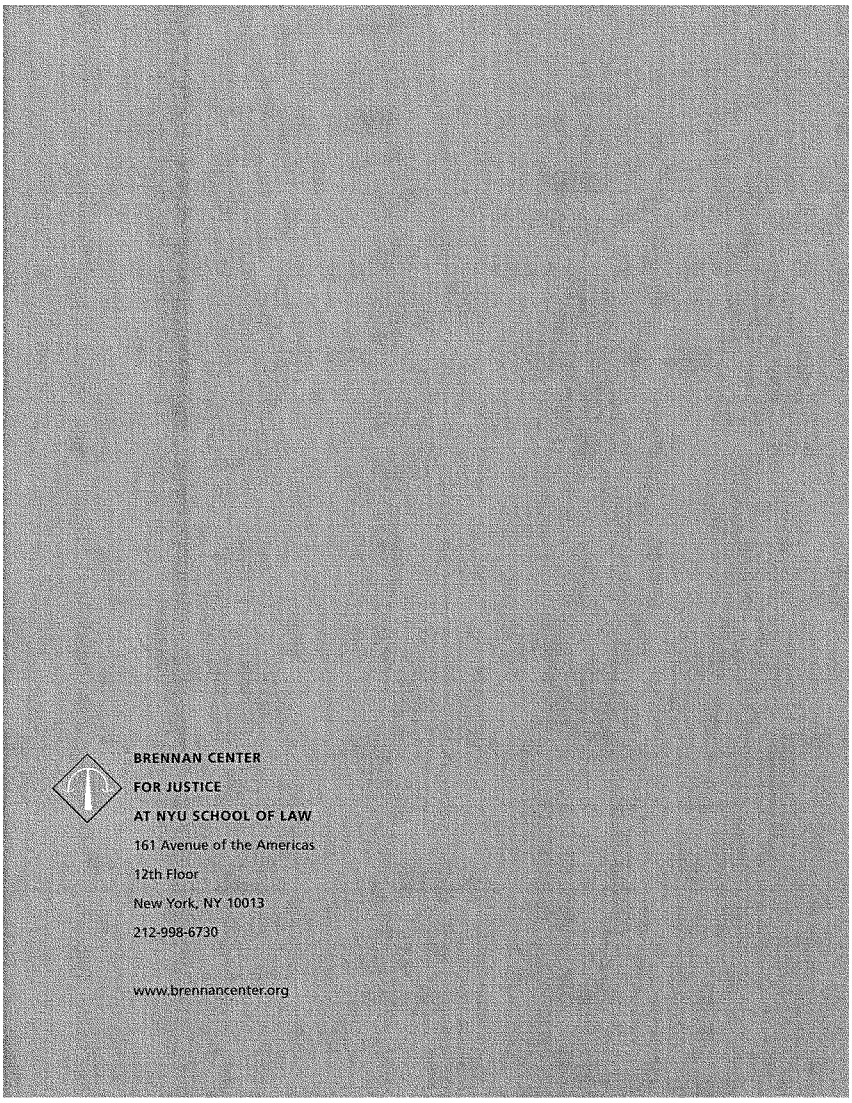
Adam Winkler
Professor, UCLA School of Law

Paul Lightfoot, Treasurer
President & CEO,
AL Systems, Inc.



BRENNAN CENTER
FOR JUSTICE
AT NYU SCHOOL OF LAW
161 Avenue of the Americas
12th Floor
New York, NY 10013
212-998-6730

www.brennancenter.org



BRENNAN CENTER
FOR JUSTICE
AT NYU SCHOOL OF LAW
161 Avenue of the Americas
12th Floor
New York, NY 10013
212-998-6730

www.brennancenter.org

MEMORANDUM ON VOTING UNIT PERFORMANCE
(Prepared by John T. Willis, School of Public Affairs, University of Baltimore)

We are as far away as a state can be from the 2000 debacle in Florida where 175,655 people did not have a vote recorded and counted for president or the 2004 controversies in Ohio where 94,535 people did not have a vote recorded and counted for president. The administration of elections in Maryland stands in stark contrast to these states and performs well above national averages. In fact, in the 2004 presidential election, Maryland ranked **number one** (***the best state***) in capturing voter intent. It is important for the public, as well as public policy decision-makers, to be aware of, and keep in mind, that:

1. There is **no** evidence (***NONE***) of the negligent, unintentional or intentional loss of votes, the failure to capture voter intent or the inaccurate compiling and tabulating of votes in the administration of elections during the 2002 and 2004 election cycles in which the existing direct recording electronic ("*DRE*") voting system was utilized.

2. Mandating a statewide optical scan voting system will **increase,** not decrease, the number of voters that do not have their votes accurately recorded and counted in the 2006 election cycle. Depending upon voter turnout, at least between **3,000 and 4,000 more** voters ***will not have their votes counted*** with a required optical scan voting system.

3. Out of 2,394,207 Marylanders who cast a vote in the 2004 presidential election **only** 7,539 did not have a vote captured or recorded for President. The resulting residual vote rate of ***0.31%*** was **the lowest ratio in the country!** (See Exhibit 1, *"Residual Vote in the 2004 Election,"* CALTECH/MIT Voting Technology Project, February 2005.)

4. The 2004 residual vote in Maryland represented the ***lowest number*** and ***lowest ratio*** of individuals not having a vote counted for the candidates running for the highest position on the ballot ***in the history of Maryland*** for any election for which comparable data is available.

5. The Maryland 2004 residual vote rate was **50%** to **seven times less** than the residual vote rate in states relying entirely, or substantially, on optical scan voting systems.

6. With 454,118 less registered voters casting ballots in the 2000 presidential election (when 19 counties utilized an optical scan voting system) there were 3,363 more voters not having a vote recorded for President than in the 2004 presidential election. The 2000 residual vote ratio was **two-thirds higher** than the 2004 ratio (when all counties and Baltimore City were using a direct recording electronic voting system).

7. The precinct level differentials in residual vote rates between voting systems are clearly manifested in comparative scatter diagrams depicting the residual vote percentage rates in Baltimore County for the 2000 presidential election using the ES&S OpTech III P optical scanning voting system and for the 2004 presidential election using the Diebold AccuVote TS direct recording electronic voting system.[1] There were only four precincts in 2004 with a residual vote rate of 1.0% or greater whereas there were 28 such precincts in 2000. Conversely, in the 2004 presidential election, 83.18% of the precincts had a residual vote rate of less than 0.5% compared with only 43.8% in the 2000 presidential election.

8. Voters in five Maryland jurisdictions comprising 42.8% of the state's total registered voters (51.4% of Democratic registered voters, 26.1% of Republican registered voters and 43.5% of other registered voters) **have never used** an optical scanning voting system at the polling place on election day. (These jurisdictions are Allegany County, Baltimore City, Dorchester County, Montgomery County and Prince George's County.)

9. Direct recording electronic voting systems are more accessible for people with disabilities, are better able to accommodate language barriers, provide for ballot magnification for voter convenience, substantially reduce residual vote variances among precincts with differing demographic characteristics, and **reduce—not** increase—the potential for voter error.

10. Any voting system used for recording and tabulating votes is subject to unintentional error and theoretically subject to intentional tampering—including, and most especially, hand counting. There was substantial justification in 1955 for the Maryland General Assembly to mandate the use of mechanical level voting machines and to bar the use of paper ballots at the polling place based upon decades of proven problems with the handling and marking of paper ballots. No such justification exists today for mandating a change in Maryland's voting system. It should also be noted that the rate of voter error and the percentage of "no votes" is higher with absentee ballots than with the use of the Maryland direct recording electronic voting system.

11. Endeavoring to change a voting system statewide in less than six months ignores the reality of the administration of elections. The procurement process for acquiring and testing over 4,000 machines, the complex ballot preparation and printing processes for nearly 1,800 precincts, and the training of approximately 21,000 election judges on the operation of a yet to be decided voting system are significant tasks that should not be rushed and compressed into an unreasonably short period of time. There is no

---

[1] See attached Exhibit 2, *Baltimore County: % of Residual Votes by Precincts for the 2000 Presidential Election* and *% of Residual Votes by Precincts for the 2004 Presidential Election.*

reason to increase the risks associated with a seriously compressed administrative timeframe, especially when there is **NO** evidence of any negligent, intentional or unintentional failure to capture the intent of any Maryland voter using the current voting system at the polling place.

12. Contrary to the assertions made in the drumbeat of publicity generated by policy advocates, and the media proclivity to report controversy, independent survey research in Maryland and elsewhere in the country has found a high degree of voter satisfaction and trust with direct recording electronic voting systems.

The public discussion about voting systems, should be informed by the Memorandum Opinion of the Circuit Court of Anne Arundel County, dated September 1, 2003. In denying the Plaintiff's Motion for Preliminary Injunction, the judge stated in pertinent part: *"All experts agreed the use of paper ballots is the least accurate of all systems and lends itself to the most chicanery. On the other hand, the experts seen to agree, if untampered, the Diebold-type voting machines are the most accurate in recording and counting votes."* The judge further observed that the fears of tampering of machines before, during or after the election *"can reasonably be protected against by implementing some of the more reasonable suggestions of the SAIC, Hopkins and RABA reports."*

During the conduct of the 2004 presidential elections in Maryland, election procedures were designed and implemented to ensure the integrity of the election. These included parallel testing of randomly selected voting machines--which in every instance confirmed the accuracy of the voting system and outperformed hand counting of the same ballot choices. In six counties, there were pre-election demonstrations and testing of the DRE voting system (Allegany, Anne Arundel, Baltimore, Calvert, Howard and Talbot). On election day, randomly selected voting units from Montgomery County were subject to parallel testing under a program designed in conjunction with the League of Women Voters. The anecdotes, allegations, theoretical abstracts and exaggerated rhetoric used to attack the voting system currently used in Maryland are not rooted in any factual examination of the performance of the voting system in actual elections in Maryland.

Can and should there be improvements made in direct recording electronic voting systems? ***Yes, and of course!*** For a significant fraction of the cost of replacing the voting system currently being used in Maryland, technological enhancements and additional technical, management and operational security measures can be taken to continue to assure a complete and accurate counting of votes in Maryland. It is important to expand the capacity to perform scientific based accuracy and logic testing and to conduct parallel testing of the voting system before, during and after any election. It is also reasonable and prudent for Maryland to continue searching for the best technology to capture voter intent fully and accurately as there will no doubt be continued improvements made in the industry. Controlled testing of new products to improve voter interface and exploring methods to enhance data security could be done on a limited,

precinct level basis without causing undue disruption to the statewide administration of elections.

There is a well-documented track record on the effectiveness of the various types of voting systems that have been used in Maryland--an examination of which that has been apparently lost or obscured in the current public discussion about voting systems. The *Report of the Special Committee on Voting Systems and Election Procedures* provided to the Maryland General Assembly in February 2001, contains a twenty year look at the efficacy of voting systems in Maryland. For the past 30 years, I have researched and closely examined precinct level voting patterns and voter behavior spanning the history of state elections for every level of government, type of office and ballot issues. What is demonstrable, down to the precinct level, are the differences that occur in voter performance utilizing various types of voting systems. What I have found is that direct recording electronic voting systems do a far better job capturing the intent of voters more accurately and completely than other voting systems, including optical scan systems. Further, direct recording electronic voting systems significantly reduce the variances among the residual vote rates cast at the precinct polling place and significantly lessen the differentials in residual vote rates among various demographic cohorts.

By mandating an optical scan voting system in Maryland, it can reasonably be projected (based upon past performance of voters using such systems in actual Maryland elections) that **more voters will not have** their intentions recorded correctly in the 2006 primary and general elections than if they were to use the current direct recording electronic voting system. As was painfully demonstrated in Florida, and has been experienced elsewhere (including Maryland), voters using an optical scan voting system will mismark ballots causing undervotes and overvotes and some ballots will not be read correctly by the voting system.[2] The February 2005 CALTECH/MIT Report found, with respect to the lowering of residual vote rates, *"that there may be particular gains to be had when a jurisdiction that already use optical scanners chooses to use the newest generation of DRE's."* A statewide optical scan voting system will produce more voter errors, cause the disenfranchisement of more voters and yield more contested and dubious election results than the current or future generations of direct recording electronic voting systems. The inevitable close election will see its reported official results change in a "recount" or contested election procedure as a result of voter and machine error in recording and capturing the intent of the voter. This differential in capturing, recording and tabulating voters has already occurred in Maryland jurisdictions using optical scan voting systems (including the 2002 general election involving the former Speaker of the House).

Finally, it would be prudent, before mandating any change to the exemplary manner in which the intent of the Maryland voter is captured accurately and completely, to subject any proposed replacement voting system to the same rigorous examination and

---

[2] Attached hereto as Exhibit 3 are examples of mismarked optical scan ballots that commonly occur. These samples were included in the *Report of the Special Committee on Voting Systems and Election Procedures* (February 2001) which was presented to the Governor and the Maryland General Assembly.

independent testing that has been given to the current voting system by the Maryland General Assembly and independent research entities. In such an examination you would likely find many of the same technology concerns and security issues that generated the current debate over direct recording electronic voting systems also exist with an optical scan voting system in the recording and tabulating of voter intent. In addition, you would likely find management and operational security issues present with an optical scan voting system that do not exist with a direct recording electronic voting system.

In concluding, I believe that it would be a clear multi-million dollar, ***step backwards***, not forwards, in the effort to capture voter intent completely and accurately to change our current voting system, especially only a little more than five months before an election! Maryland would no longer be a national leader in capturing voter intent and vote counting accuracy but would find its top of the list rankings decline in future election cycles. We should all continue to work toward solutions that will keep ***accurately and fully capturing the intent of Maryland voters*** as the principal goal and objective in the administration of elections in our state.

ROY G. SALTMAN, M.S., M.P.A.
Consultant on Election Policy and Technology
5025 Broken Oak Lane, Columbia, MD 21044
Phone: 410.730.4983/Fax: 410.997.4355
email: rsaltman@alum.mit.edu

Sept. 26, 2006

Honorable Vernon J. Ehlers, Chairman
Committee on House Administration
US House of Representatives
1309 Longworth House Office Building
Washington, DC 200815-6157

Dear Representative Ehlers:

I am writing to you about the subject of your committee's hearing on September 28, 2006, that is, electronic voting machines: verification, security, and paper trails. I request that this letter be placed in the hearing record.

This letter summarizes my recent report on this subject. The final text of the report, entitled Independent Verification: Essential Action to Assure Integrity in the Voting Process," was submitted to the National Institute of Standards and Technology (NIST) under contract on August 22 and has been made available on a NIST website. I handed a paper copy of the report to Paul D. Vinovich, the committee's director of legislative operations, on September 22. The report represents my personal views, conditioned by my thirty years of research and publication on this subject.

My recommendation is that audits must be carried out on all officially reported results of federal elections, regardless of the type of voting technology. Public confidence in the democratic process requires this action. When direct-recording electronic (DRE) voting machines are used, independent ***electronic*** audit trails must be implemented on each machine and used to verify the reported results. When hard-copy ballots are employed, the percent of precincts independent verified should increase proportionally with the narrowness of the winner's victory but, in any event, should include, automatically, at least 3% of all precincts at no cost to the loser. Precincts whose results generate the most doubt should be selectable for recounting by the losing party or candidates.

My report points out difficulties with the paper-printout system now being mandated in many states for use with DRE voting machines. These unacceptable attributes are:

(1) Visually handicapped voters cannot read these printouts; advocates for the blind have filed lawsuits claiming that the use of the printouts violates HAVA requirements for equal access.

(2) A majority of sighted voters are not reviewing their printouts, with the result that the printouts not reviewed remain the product of untrusted computer programs.

(3) A reason for the non-review is the extra time required by the voter, extending the duration of voting after the process has been essentially completed.

(4) The printout is not presented in the same format as the electronic screen, resulting in a

voter-unfriendly and difficult comparison.

(5) Loss of privacy may result from the sequential spooling of the printouts, and the discovery of an incorrect computer program by a voter demands that the voter violate the state's guarantee of privacy.

Commercial products have been devised that provide for copying of the voter's final screen on a DRE to a separate computing device. This procedure allows for the independent recording, summation and disclosure of election results by electronic means instead of paper. The voter need not have any personal hand in this process, thereby eliminating any required additional activity on the voter's part and eliminating any activity not able to be carried out by voters with handicaps. Additional products of this type are likely to be produced in the near future, as the technology is not unusual, prohibitively intricate or expensive. My report recommends that such devices, if employed, must have their software publically disclosed, and must be approved for use through the testing process of the accredited Voting System Testing Laboratories.

In this letter, I have shown that the public can have confidence in reported election results without the use of paper. My hope is that the Congress will not restrict the future use of technology by an insistence on paper, at a time when nearly all organized business and government operations are attempting to eliminate paper.

However, I have asked that actual audits be required to be carried out, which is not a current requirement. If elections are to be carried out in an efficient, effective, and "business-like" fashion, then audits must be undertaken. Every business of significant size in this country is required to carry out independent audits, for the benefit of investors, regulatory agencies, and taxing authorities. Certainly, the results of public elections are as worthy of public confidence as the financial condition of private corporations.

Sincerely,



Roy G. Saltman

DIEBOLD
ELECTION SYSTEMS

Diebold Election Systems Response to the Princeton University AccuVote-TS Analysis

The following statement may be attributed to Dave Byrd, President, Diebold Election Systems.

September 13, 2006 – "Three people from the Center for Information Technology Policy and Department of Computer Science at Princeton University today released a study of a Diebold Election Systems AccuVote-TS unit they received from an undisclosed source. The unit has security software that was two generations old, and to our knowledge, is not used anywhere in the country. Normal security procedures were ignored. Numbered security tape, 18 enclosure screws and numbered security tags were destroyed or missing so that the researchers could get inside the unit. A virus was introduced to a machine that is never attached to a network."

"By any standard - academic or common sense - the study is unrealistic and inaccurate."

"The current generation AccuVote-TS software – software that is used today on AccuVote-TS units in the United States - features the most advanced security features, including Advanced Encryption Standard 128 bit data encryption, Digitally Signed memory card data, Secure Socket Layer (SSL) data encryption for transmitted results, dynamic passwords, and more."

"These touch screen voting stations are stand-alone units that are never networked together and contain their own individual digitally signed memory cards."

"In addition to this extensive security, the report all but ignores physical security and election procedures. Every local jurisdiction secures its voting machines - every voting machine, not just electronic machines. Electronic machines are secured with security tape and numbered security seals that would reveal any sign of tampering."

"Diebold strongly disagrees with the conclusion of the Princeton report. Secure voting equipment, proper procedures and adequate testing assure an accurate voting process that has been confirmed through numerous, stringent accuracy tests and third party security analysis."

"Every voter in every local jurisdiction that uses the AccuVote-TS should feel secure knowing that their vote will count on Election Day."

Contact:
Mark Radke, Director of Marketing, Diebold Election Systems, 330-490-6633

ELECTION SYSTEMS

Diebold Election Systems, Inc.
P.O. Box 1019
Allen, TX 75013
www.dieboldes.com

Diebold Responds to RFK, Jr. and Rolling Stone

Allen, Texas - Diebold Election Systems today released the following letter to the editors of *Rolling Stone* magazine. The letter responds to an error-riddled piece authored by Robert F. Kennedy, Jr. and published in the magazine.

Mr. Kennedy did not contact Diebold Election Systems for comment, despite the fact that they are the primary target of Mr. Kennedy's article which draws on the claims of a former Diebold employee who was removed at the request of the Georgia Secretary of State.

Diebold Election Systems is calling on *Rolling Stone's* editors to review the critical facts below and disavow the shoddy reporting done by Mr. Kennedy.

September 26, 2006

Mr. Jann Wenner
Editor and Publisher
Rolling Stone
1290 Avenue of the Americas
New York, NY 10104 - 0298

Subject: "Will The Next Election Be Hacked?"

Mr. Kennedy should have made serious efforts to verify the validity of his article's sources and assertions. He did not even contact Diebold Election Systems for comment. In doing so, he would have learned that his so-called whistleblower undermines his own case, and the claims he makes fail to hold up under bright light of the truth.

The whistleblower in this article was not involved in the system implementation in Georgia for the duration he claims. On July 23, 2002, the Georgia Secretary of State's office directly requested that Mr. Hood be removed from his duties as a voter outreach instructor because of poor performance. This request is clearly documented in a letter from the Secretary of State's office, which is attached.

After a review of the facts provided below, we believe you will come to the determination that this story falls short of serious journalistic standards.

We're in the business of supporting our democracy, so our credibility and independence is imperative. While we're reluctant to be perceived as entering the political fray, we feel compelled to address in a vigorous and factual fashion these false accusations, which foster fear.

Mr. Hood, a.k.a., the whistleblower, was a contractor for Diebold in Georgia and was to conduct a voter outreach program in the state of Georgia. However, as stated in a letter dated July 23, 2002, the Secretary of State's office requested the removal of Chris Hood from his role working in the state. The letter reads, in part:

> "In light of the limited timeframe, resources and opportunities that we have to contribute to the success of the nation's largest electronic voting deployment, we are requesting that a more appropriate resource be provided to support a fully coordinated voter education effort. With that perspective in mind, it is our position that Mr. Hood and his organization are not providing maximum benefit in their services to the State of Georgia in our efforts to help educate Georgia voters about the new voting system. Therefore, we respectfully request that Diebold Election Systems, Inc. review the current assignment of resources and make the appropriate changes necessary for the State of Georgia to achieve its voter education goals." Michael Barnes, Assistant Director of Elections.

Immediately upon receiving this letter, Diebold Election Systems removed Mr. Hood from his responsibilities within the state. He no longer contributed to the implementation process in Georgia. Yet the allegations contained in Mr. Kennedy's article make it appear as if Mr. Hood were there and working with the system on a daily basis.

For example, Mr. Hood mischaracterizes the "patch." The patch was an operating system modification, not a modification to the tabulation system as implied in this article. This modification was not completed and available for installation until after August 8, 2002, at least two weeks after Mr. Hood was removed from his position in Georgia. Clearly, his reference, "We ran the election," is not factual.

There are additional errors and inconsistencies in Mr. Hood's claims and throughout Mr. Kennedy's article:

"We were told that it was intended to fix the clock in the system, which it did not do," Hood says. "The curious thing is the very swift, covert way this was done."

First of all, Mr. Hood was not even working on the project at the time. Secondly, the election review panel within the state of Georgia reviewed the operating system software before implementation. It was not done covertly, as alleged by Mr. Hood.

"It was an unauthorized patch."

Again, this statement is wrong. Modifications to the operating system of the units did not require federal certification. However, complete logic and accuracy testing on every unit was implemented by the respective jurisdictions following insertion of the modification to insure system accuracy.

"Diebold also illegally installed uncertified software in machines used in the 2004 presidential primaries."

Diebold Election System software used during the 2004 presidential primary was certified by the Federal Election Commission organization and/or approved by the chief election official within each respective state.

"Diebold, along with its employees and their families, has contributed at least $300,000 to GOP candidates and party funds since 1998."

Diebold's ethics policy restricts top executives of the company and all members of the election system division from participating in fund raising activities. This was instituted in June of 2004.

"Diebold not only failed to follow up on most of the recommendations, it worked to cover them up. Michael Werthheimer, RABA"

A series of security enhancements have been added to the Diebold touch screen machines based on the RABA report. They include: Advanced Encryption Standard (AES) 128-bit data encryption, dynamic passwords, and digitally signed memory card data.

"That year (2004), Diebold would count the votes in half of Ohio's counties."

Not a single Ohio jurisdiction deployed Diebold Election Systems' touch screen system during the 2004 presidential election. None. Zero. Two of Ohio's eighty-eight counties used the Diebold Election Systems paper ballot optical scan system. The larger of the two counties, Lucas County, overwhelmingly voted for John Kerry. The article contains additional fabricated information.

"The three counties with the most discrepancies - Broward, Palm Beach and Miami Dade – were also the most heavily Democratic"

None of these three counties use Diebold Election Systems voting equipment.

As regards the Princeton study referenced in the article, our response to this deeply flawed report can be found at the following address:
http://www.diebold.com/dieboldes/pdf/princetonstatement.pdf

"On September 12th, in Maryland's first all-electronic election, voters were turned away from the polls because election officials had failed to distribute the electronic access cards needed to operate Diebold machines."

An election official's human error of not loading voter access cards into the supply bags for the precincts is now absurdly being portrayed as a system-related problem. This issue is analogous to an election official forgetting to send paper ballots to a precinct. It is human error -- not system error.

"Electronic voting machines are making things worse instead of better."

The author of the Cal Tech/MIT study, Charles Stewart III, who is also quoted in the *Rolling Stone* article indicates in this report that with the implementation of new voting equipment and procedures, "this works out to a recovery of one million "lost votes" between 2000 and 2004." This certainly indicates a dramatic improvement in voting accuracy.

"A government report uncovered large and unexplained discrepancies in vote totals recorded by machines in Cuyahoga County."

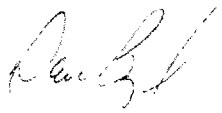
The ESI report was proven to be in error by the Cuyahoga County Board of Elections, as archived election data exactly matched official election results once the errors of the ESI report were identified by the board and corrected. As an example, 17 year old and curbside votes were not included in the studies' analysis, but of course were included in the official election totals. The Cuyahoga County Board meeting minutes disclose this fact.

"The company had barely completed its acquisition of Global Election Systems" (date referenced is May 2002).

The Global Election Systems acquisition was completed by Diebold on January 22, 2002.

Don't the readers of *Rolling Stone* deserve a better researched and reported article than the one penned by Mr. Kennedy? We think so. We hope that after reviewing this letter *Rolling Stone* will agree.

Sincerely,



David Byrd
President

DIEBOLD

Diebold Election Systems, Inc.
PO Box 1019
Allen, TX 750013

Michael E. Lindroos
Vice President
LindroM@Diebold.com
330-705-7654

August 16, 2006

Cuyahoga County Commisioners
Administration Building
1219 Ontario Street
Cleveland, Ohio 44113

Via email and regular mail

Re: Erroneous Report Posting

Dear Commissioners Hagan, Commissioner Dimora and Commissioner Lawson Jones;

We are surprised and dismayed by the posting of the Election Science Institute-ESI (VoteWatch) inaccurate analysis covering the May 2006 primary election (the "Report"). The Report is inaccurate and the result of an erroneous and misleading investigation that is clearly false.

We have previously pointed out the errors in the Report and the investigation methodology to the County. We have further been made aware that the County also informed ESI of these defects on August 3rd. The Report as posted fails to take our comments into account or correct the defective analysis. Attached is a document reflecting a more accurate description of the issues which were inaccurately portrayed in the Report. Such document is incorporated herein by reference. We would request that the Report be immediately removed from the County's website, and a copy of this letter and the attachment be distributed to all persons who have received the same from the County. Such distribution should at least be by means of posting this letter on such website in lieu of the Report.

We believe that the continued publication of the Report without including our comments can be reasonably interpreted to constitute intentional and willful defamation of Diebold Election Systems.

Given the pre-Report unwillingness of ESI to allow Diebold Election Systems to participate in the analysis of the election specific data prior to the report and the evaluation of the specific election equipment, there would seem to be an apparent weakness in the skills of ESI or the investigatory methodology employed by them in this instance. This is especially true due to the simplistic analytical errors which were discovered independently by both the County's election professionals and Diebold Election Systems. Quite frankly, given the weakness of this analysis, we feel it would be irresponsible for any jurisdiction to rely on the reports such as this by ESI without a very thorough review of their background, the work performed and the analytical methodology utilized.

Diebold Election Systems equipment is reliable and accurate. This has been demonstrated in not only all other Ohio jurisdictions using the system during the May primary, but also in thousands of elections in hundreds of jurisdictions throughout the nation. One example of independent evidence of the accuracy of our equipment can be found in the parallel monitoring testing conducted by the State of California in actual elections over the past several years.

We look forward to your taking action consistent with the requests found in this letter.

Sincerely,

Michael E. Lindroos, Esq.
Vice President and Counsel

cc: Mr. Michael Vu, Director of Elections, Cuyahoga County
Mr. Hertzberg, ESI
Mr. David Byrd, President, Diebold Election System
Ms. Jessica Hiner, Diebold Election Systems
Mr. Hugh Shannon, Cuyahoga County Commissioners

August 15, 2006

Response from Diebold Election Systems to the Election Science Institute Report to the Cuyahoga County Board of Commissioners re: the May 2006 Primary Election

Background: The Cuyahoga County Board of Commissioners contracted with Election Science Institute (ESI) to analyze various aspects of the May 2006 Primary Election. ESI's initial report was presented to Cuyahoga County officials on Friday, August 11, 2006. Diebold Election Systems has reviewed that report along with the Cuyahoga County Board of Elections. The following response can be attributed to Mark Radke, director of marketing, Diebold Election Systems.

++++++++++

"The initial review and conclusions reached by ESI concerning the Comparison of Vote Count By Candidate simply are wrong. In their primary areas of focus, ESI failed to take into account Election Day administrative actions that – had a thorough analysis been done and questions asked – would have determined the correct answers. The county provided additional data to ESI on August 3rd when ESI was unable to reconcile the two analysis databases. This data from the county was not incorporated into the ESI report and their conclusions within this report are incorrect. The Cuyahoga County Board of Elections and Diebold Election Systems again reviewed the analysis databases on August 12th, and confirmed the initial data provided by the county on August 3rd. In some cases, it is apparent that ESI itself made mistakes in its own testing procedures.

"The principal issues are the seeming discrepancy between the memory cards and the Voter Verifiable Paper Audit Trail (VVPAT) totals, and the on-the-surface mismatch between the precinct memory cards and the touch screen unit's internal memory totals. However, the actual vote results can be balanced and verified when the Election Day administrative actions are incorporated into the analysis.

"As previous reviews have shown, poll worker training was insufficient. Poll workers in various locations apparently pulled memory cards from one touch screen unit and placed that memory card into another touch screen unit. However, they did not also remove the respective VVPAT paper tape and place it into the second unit. Clearly, removing a memory card from one unit and placing it into another without also relocating the VVPAT records will account for a discrepancy when those results are compared.

"In addition, several precinct locations called the Cuyahoga County election office early on Election Day to report they did not have memory cards for their touch screen units. New memory cards for the precincts were programmed at election center and delivered to the respective precincts. In the meantime, poll workers found the original memory cards and began to use them in the touch screen units. When the new memory cards arrived from election central, the original cards were removed and the new cards were inserted into the touch screen units and used for the remainder of the election. This type of memory card activity will cause totals from the individual memory cards and the touch screen unit not to match.

"ESI's review failed to take into account the procedures for handling curbside voters and 17-year old voters. As a result, the report erroneously concludes that precinct totals from specific precinct or voting center memory cards do not match the totals from the touch screen unit's internal memory located on the unit's motherboard. Cuyahoga County used paper ballots for these special voting cases. The votes were inputted into touch screen units and the totals were placed on separate memory cards. It is apparent that ESI tabulated the memory card totals from the touch screen units used within the precinct for walk-in 18 year and older voters, but did not include the totals from the memory cards for curbside voters or 17-year old voters. This omission caused the variance between the two totals. The Cuyahoga County Board of Elections notified ESI of this omission on August 3rd.

"ESI's own testing procedures also were flawed. On several memory cards which were uploaded by ESI from the touch screen unit's internal memory and used for the ESI analysis, zero votes were present;

however, the internal memory of the touch screen units contained between 30 and 50+ votes, respectively. The original memory cards used in these touch screen units during the actual election contained the same number of votes as the internal memory of these units. ESI operator error appears to be the cause of these memory cards used in the ESI analysis not containing any votes, as they should have been uploaded directly from the touch screen's internal memory which did contain the correct number of votes cast. ESI does state in the analysis that "Human error can not be ruled out as the source of the discrepancies reported."

On page 88 of the ESI analysis, it states, "Printer problems were not evenly distributed throughout but rather were clustered in particular voting centers. For example, 18 voting centers experienced 100% of the printer errors (4 vote centers experienced 46% of the printer errors)." Clearly, poll worker training was an issue in these specific precincts, as the VVPAT printer performed admirably in the vast majority of precincts.

"Finally, the ESI report (Page 100) criticized the VVPAT's performance because the ink occasionally ran low, even though the VVPAT does not use ink or an ink cartridge. A thermal printer is used within the VVPAT to eliminate the issues associated with replacing ink cartridges. Thermal printers also require virtually no maintenance and are very reliable, as heat is used in place of ink to mark the VVPAT paper.

"The accuracy and reliability of Diebold's system is proven as the system has been tested by federal and independent laboratories, and has passed a regime of stringent parallel monitoring accuracy tests. Diebold Election Systems will continue to work with the Cuyahoga County Board of Elections staff to address any perceived issues that arise so that the November General Election can be conducted smoothly, as was the case with the August special election."

Election Officials Pleased
Electronic Machines Found Reliable

August 23, 2006 **CONTACT: Aaron Ockerman**
FOR IMMEDIATE RELEASE **(614) 581-8238**

COLUMBUS, OH- After the results of an audit of the Cuyahoga County primary were found to be faulty, election officials around Ohio again sought to assure their voters that their votes will be counted.

"As we had stated previously, the audit in Cuyahoga County provided no reason for voters to question the integrity of their elections process or the machines that record their votes," said Steve Harsman, President of the Ohio Association of Election Officials (OAEO). "Those of us who do this for a living knew immediately that something was wrong with the study, and it disheartened us that so many people used it as an excuse to try and erode the public's trust in our elections system," he continued.

After vendors and election officials were brought in to discuss the findings of the study which cast aspersions on the safety of the voting equipment, many gaps were found in the results. Claims that vote totals on memory cards did not match up to vote totals on paper trails were found to be untrue. After further analysis, it was proven that no votes were lost, and other than minor problems with paper jams, the equipment performed as expected.

Jeff Matthews, past president of the OAEO, attributed poor execution of the audit for the problems. "Unfortunately, ESI either didn't know how Ohio's elections systems worked, or chose to ignore their own people who tried to advise them of it. Their methodology was flawed, their execution was poor, and their results and conclusions suffered as a result. The real losers of this non-accredited agency's debacle are the voters of Ohio who were given false conclusions and made to believe that their elections are unsafe."

More than 40 Ohio counties have now used electronic voting equipment in elections, and most counties have had a smooth conversion from their old equipment. While no transition of this magnitude unfolds without problems, all parties seem to be moving forward without major incident. Voters appreciate the ease of use of the new machines, and election officials continue to gain experience and expertise with their new equipment.

Harsman added that his own experience in Montgomery County validates that the new voting technology does work. "My staff has worked 18 hour days seven days a week to prepare for our elections, and the results have been fantastic. With proper training, solid processes, and a little elbow grease on our part, Ohio's elections can continue to be top notch," he stated. "I think the bottom line of this whole mess is that the problems experienced in Cuyahoga County are fixable and isolated. Attempts to use their experience to condemn the entire state just don't hold water," he concluded.

The Ohio Association of Election Officials is a bipartisan organization representing the members of Ohio's 88 county boards of elections, their directors and deputy directors. OAEO is a professional organization dedicated to the training and education of its members, thus ensuring fair and accurate elections for all Ohioans. Steve Harsman, President of the OAEO, is director of the Montgomery County Board of Elections. Jeff Matthews, past president of the OAEO, is Director of the Stark County Board of Elections.

-30-

From: Rebecca Mercuri, Ph.D.
To: The U.S. Congressional Committee on House Administration
Subject: Electronic Voting Machines: Verification, Security and Paper Trails
Date: October 4, 2006

I am submitting this comment on the subject of "Electronic Voting Machines: Verification, Security and Paper Trails" with the request that it be added to the record of the hearing held on September 28, 2006 by the Committee on House Administration.

I, Rebecca Mercuri, am the President and Chief Technology Officer of Notable Software, Inc., of Mercer County, New Jersey, a computer consulting firm I founded in 1981. I have been researching electronic balloting systems since 1989, and defended my Doctoral Dissertation, entitled "Electronic Vote Tabulation: Checks & Balances," at the University of Pennsylvania's School of Engineering and Applied Sciences, on October 27, 2000. In addition to my Ph.D., I have two Master's degrees and a Bachelor's degree in Computer Science and Engineering. During 2003-2005 I held fellowship positions at Harvard University, first at the John F. Kennedy School of Government, and then at the Radcliffe Institute for Advanced Study. I am the sole author or primary co-author of over 40 published technical papers, nearly half of which have pertained to electronic balloting or vote tabulation. My writings on this subject have been cited in the U.S. Congressional Record and on the floor of the Irish Parliament. I have also delivered comments upon request to the U.S. House Science Committee, the U.S. Commission on Civil Rights, the U.K. Cabinet's Office of the e-Envoy, the Federal Election Commission, the U.S. General Accounting Office, State Legislative Committees in Connecticut, Pennsylvania and North Carolina, the New York State Board of Elections, and numerous municipal boards. I have had a direct role in influencing the wording pertaining to paper ballot records that appears in the Help America Vote Act (HAVA) and many state election laws. I served for three years as a member of the Institute for Electrical and Electronics Engineers' working group that provided material incorporated into the Election Assistance Commission's 2005 voting system guidelines. Some of the activities that I have performed during the course of my investigations and research have included: casting sample votes on a wide range of balloting systems (including use of accessibility features), attending detailed briefings on the operation and set-up of this equipment, communicating with numerous election company officials, technical and sales personnel, and reviewing equipment certification reports from various states.

When I appeared before the U.S. House Science Committee at their May 22, 2001 Hearing on "Improving Voting Technology: The Role of Standards," among my statements was the following:

> "To date, no electronic voting system has been certified to even the lowest level of the U.S. government or international computer security standards (such as the ISO Common Criteria or its predecessor, TCSEC/ITSEC), nor has any been required to comply with such. No voting system vendor has voluntarily complied with these standards (although voluntary compliance occurs within other industries, such as health care and banking), despite

> the fact that most have been made aware of their existence and utility in secure product development."

Over 5 years later, the above statement continues to remain true. Electronic voting systems are less secure and less reliable than any computer-based systems that are deployed in applications where auditability is mandated by law. Why this is so, is (at least in part) because of certain loopholes in the Federal Voluntary Voting System Guidelines (VVSG) that first appeared in the Federal Election Commission (FEC) document set, and were perpetuated into the FEC 2002 and EAC/HAVA 2005 sets, despite vigorous and increasing protest by the scientific and engineering community.

In particular, all versions of the VVSG specify a Mean Time Between Failures (MTBF) rate that allows for many equipment malfunctions during election day to be deemed "within specifications" even when they affect up to 10% of the voting units. Such malfunctions can result in voter disenfranchisement, as we have recently seen in Maryland and elsewhere. This astonishing inadequacy (publicly noted by Dr. Stanley Klein to the EAC in 2004) explains why Cuyahoga County Ohio may have experienced a 10% rate of failure with their Voter Verified Paper Audit Trail (VVPAT), and also why their vendor has not been held accountable for such poor performance. In this day and age, there is absolutely nothing that constitutes rocket science when it comes to printing information on pieces of paper in a reliable fashion. For example, the Diebold company manages to successfully print millions of pieces of paper each day, at their Automated Teller Machines located around the globe. As well, in 4/5 of the U.S. States, millions of lottery tickets are successfully printed, in a secure and anonymous fashion, every single day. But when it comes to voting, instead of using reliable paper printers that can perform a "cut and drop" action following ballot review by the voter, all of the major election system vendors have deliberately chosen to implement VVPATs by using flimsy reel-to-reel paper that violates voter privacy in addition to failing at the rate "deemed allowable" by the Federal standards. It is my belief that this "design for failure" of the VVPATs has been intentionally and deliberately used to undermine the numerous state laws that have been enacted in this regard, and to enable such anti-VVPAT showboating as was displayed by some of the panelists at your hearing on September 28th.

Certainly, Direct Recording Electronic (DRE) voting machines do not have to produce VVPATs on long, thin strips of thermal paper. The VVPAT could take the form of a Voter Verified Paper Ballot (VVPB), such as the optically scanned ballots, used by 60% of U.S. counties and an increasing number of "absentee" voters. The AutoMark <http://www.vogueelection.com/products_automark.html> is one such product that allows a full range of disability access in the private preparation of an optically scanned paper ballot that is essentially the same as those prepared manually by voters who do not require computer assistance. The Vote-PAD <http://www.vote-pad.us/> is a mechanical system that also allows disabled voters to privately prepare an optically scannable VVPB.

Another area of great concern involves the security vulnerabilities of computer equipment used in ballot preparation and vote tabulation. Here again, the federal agencies responsible for creating voting system guidelines have continued to perpetuate a loophole

that poses a serious risk, that of the blanket exemption from inspection for Commercial-Off-The-Shelf (COTS) software and hardware. As I, and colleagues Vince Lipsio and Beth Feehan, wrote in an article to appear in the November 2006 Communications of the Association for Computing Machinery:

> "This loophole is anathema to security or integrity. In other critical computer-based devices (e.g., medical electronics or aviation) COTS components may be unit tested a single time for use in multiple products, with COTS software typically integration tested and its source code required for review to ensure that it is indeed unmodified. In contrast, for voting equipment, this blanket inspection exemption persists, despite having strenuously been protested by numerous scientists, especially in the construction of guidelines authorized by the Help America Vote Act (HAVA). Nevertheless, special interests have prevailed in perpetuating this serious backdoor in the advisory documents used for the nation's voting system testing and certification programs."

Another massive security loophole that is allowed by the EAC/HAVA voting system guidelines involves the use of telecommunications devices to provide access to critical data for voter authentication, ballot definition, vote transmission, vote count, and voter lists. Although Dr. Felten has demonstrated that computer viruses can be transferred to voting equipment even when network connectivity is not present, the EAC showed an astonishing lack of discretion when it authorized that voting systems could be connected "across a broad range of technologies, including, but not limited to: wireless, microwave, public telecommunications lines, and communications routers." I informed the EAC on September 30, 2005 that "all such channels are not only highly vulnerable but provide avenues for insider as well as extensive outsider exposure to the election data and also potential access to the object code versions of the software running within the balloting and vote tabulation equipment. There is absolutely nothing in the standard that provides any real confidence or confirmation that accuracy, durability, reliability, availability, and integrity can be maintained for voting systems interfaced to telecommunications environments." This is especially true where there is no means provided whereby voters and election officials can independently verify the correctness of electronically recorded ballots and their subsequent vote totals. Nevertheless, the EAC has deemed that this serious connectivity risk may persist.

As flawed as the 2005 EAC standards are, they are still an improvement over the earlier FEC ones that ignored making any implementation recommendations regarding VVPATs. Since the EAC standards were also issued late, absolutely none of the $3B in HAVA funds will have been spent on "HAVA certified" equipment. Instead, these purchases were made for 2002 and even 1990 certified systems, some of which also fail to adequately satisfy the HAVA disability requirements. As early as 2003, I was publicly calling for a moratorium on all DRE purchases for these reasons. Although the EAC granted an extension for submission of the HAVA state plans, and could have (with the cooperation of Congress) similarly authorized an extension for the equipment purchases until the HAVA voting products were certified and available, this was not done. As Chairman Vernon Ehlers correctly noted in his closing remarks to this panel, and as I

have also often said, it is unfortunate that the "cart was placed before the horse" in not requiring that adequate standards were fully in place before the funds were allocated. The result is that the vendors have received a cash bonanza to, in effect, move their "used cars off of the lot," so to speak. Some years down the road, when the new equipment models arrive, no HAVA funds will be left to be spent on them. Nor will any Federal funds be available to compensate communities for replacement of the malfunctioning and inadequate equipment that has, unfortunately and unwisely, been purchased under the HAVA program.

The EAC needs to immediately close the aforementioned loopholes that exist in the voting system guidelines. This can best occur if the voices of scientists (such as myself) who have made extensive contributions to the understanding and deployment of verified voting technologies, and members of the disability community who are not opposed to VVPATs, can be heard. The current exclusionary practices, especially those that display vendor influence and bias, in these official discussion forums must be ceased.

It is not too late to provide all citizens of the United States with the ability to independently verify that the ballots they cast in the 2008 Presidential election have been recorded as they intended. And it is not too late to provide all election officials with voting systems that enable efficient and proper audits of election results without the use of computers. Presently, this is only possible with paper. For now (November 2006 through 2008's election cycles), the only appropriate recommendation that can be made is to allow communities that had obtained the DRE systems to instead provide their paper-based "absentee" ballots for use by all voters, throughout the precincts. In the future, voting system vendors should be encouraged to augment such paper-based systems with additional security controls that improve the detection of ballot alteration or removal attempts. America need not fear that a return to paper-based voting will cause us to be looked upon as Luddites, rather it should focus its attention on providing the best election technology in the world. The current crop of DRE voting machines simply do not fit the bill and should be withdrawn from use.

Respectfully submitted,

Rebecca Mercuri, Ph.D.
Mercer County, New Jersey
mercuri@acm.org
609/587-1886

COMMON CAUSE
Holding Power Accountable

Sept. 28, 2006

Statement of Chellie Pingree,
President, Common Cause

Common Cause strongly supports H.R. 550, the Voter Confidence and Increased Accessibility Act of 2005, that would require electronic voting machines to produce a voter-verifiable paper ballot.

The voting debacle in the recent Maryland primary makes clear that electronic voting machines are not ready for the critical task of casting and counting votes. But of the many problems in our system of voting, this one is fixable. Congress can move quickly to pass H.R. 550 and require a voter verifiable paper ballot with mandatory random audits for electronic voting machines and help restore voters' faith in our elections system.

Since 2003, when Representative Rush Holt (D-NJ) first introduced H.R. 550, computer security experts have almost unanimously endorsed his plan for requiring every voting machine in the United States to produce or incorporate a paper record of each voter's ballot that can be checked and verified by that voter, and used in subsequent recounts and audits.

Election experts, civil rights activists and citizens concerned about their vote have come to recognize the need for these requirements as election after election in state after state has demonstrated all too clearly the probability of voting machine malfunction.

In the past three years, a large body of research by government, academic, and corporate entities has confirmed the problems with paperless voting and has reiterated the need for voter-verified paper records and mandatory random audits. Today, 215 co-sponsors—Democratic, Republican, and Independent—stand with Representative Holt to support this legislation.

Now, it is time for Congress to act.

Testimony of Mr. Larry W. Holmstrom
Chief Executive Officer of TruVote International, Inc.

Leading Our Nation to Transparent Elections

Congresswomen and Congressmen:

It is with great pleasure I present this testimony to the committee concerning electronic voting equipment.

TruVote was formed in 2000 following the "hanging chad" election where many voters were disenfranchised due to the operation and use of our voting machines. TruVote was organized to provide solutions to this problem with the mission to insure:

> Every vote counts;
> Every vote is counted;
> Every vote accurately represents the intention of the voter;
> The voting public has confidence in the electoral system;
> The paper record, certified by the voter, is the legal representation of the vote;
> Electronic records can be audited with access to the paper ballots;
> Elections are accurate.

TruVote International believes the public should have confidence in the United States electoral process. HAVA was enacted in 2002 with the objective to upgrade voting machines and to provide assistance and guidance to the states for fair and accurate elections and to increase voter confidence in the electoral process. The resulting implementation has not achieved these goals. The dominance of electronic voting machines by one or two vendors, coupled with poorly engineered systems, lack of consideration for accuracy, and arrogant company policies has resulted in HAVA funded equipment that does not meet the expectations of the voting public.

The responsibility for election accuracy has been moved from the public domain to the domain of a private company. For example, one vendor, in their response to a state RFP responded:

> " ... How does the proposed system manage recounts and verify that the ballots accurately reflect the votes cast?...
>
> RESPONSE: This response is TRADE SECRET AND CONFIDENTIAL"

TruVote believes the United States elections should never considered private property; they belong to the public. Voting systems should be open and

transparent. Public confidence is an important foundation for our democratic processes.

Electronic voting machines are important to provide the convenience and accuracy desired by the voting public. Electronic voting machines provide the ability to present to the voter, a correct ballot face and assist them in making accurate and complete race selections. With today's electronic voting systems, the accuracy of the voter's selections are suspect without the ability to audit and subject to errors and potential malfeasance.

In contrast, the United States public uses electronic machines to successfully and accurately record over 100 million financial transaction daily. Electronic voting machines need to be held to this standard.

Key to successful and accurate financial transactions is the generation of a paper receipt. The paper receipt is certified and retained by the purchaser as proof of the transaction. This receipt, reviewed and certified at the time of purchase, is the legal transaction record. An electronic record of the transaction is also created for efficiency in accounting, but the paper record remains the legal record. If any inaccuracy of the electronic report of the transaction is suspected, the legal paper record is used to correct the transaction. We need the same processes for our electronic voting.

The focus of the electronic voting system should be the paper ballot. This paper ballot, as certified by the voter, should be the legal record of the vote. Electronic voting machines should make a corresponding electronic record of the vote and have efficient tallies and tabulations, but the paper ballot remains the legal record. **The focus should be the paper record, not the electronic record.**

This is not the case with current HAVA implementations. The term VVPAT – Voter Verified Paper Audit Trail – suggests the paper record is not the legal record but is to be used for audit purposes. The correct focus should be a **Voter Verified Paper Ballot** reflecting the paper ballot as the legal record of the vote.

The voter should be issued a receipt reflecting his or her successful voting. While it is not legal to issue a voter an actual copy of their ballot selections due to potential election fraud, the receipt should link to the paper and electronic records of the ballot selections. The voter should be able to confirm that his or her vote has indeed been counted and an audit can be or has been performed confirming the match of both the paper and electronic records.

A unique identifier should be required linking the paper and electronic records. The 2005 Voluntary Voting System Guidelines, Volume I, page 131 in discussing the requirements for voter verified paper audit trails (VVPAT) states:

> "The multiple cast vote records are linked to their corresponding audit records by including a unique identifier within each record."

In addition, audit and verification should be part of the election process. The 2005 Guidelines states in section 7.9.3(g):

> "The paper record shall be created such that its contents are machine readable"

These standards have not been met. While voting jurisdictions have mandated VVPAT capability on their voting systems and the dominant equipment vendors have claimed "VVPAT capability", they have not implemented these and other features of the standard.

If we held electronic voting machines and their use to the same standards that we expect with electronic transaction recording machines, we will restore the public confidence in our electoral process. I would like to suggest several steps Congress might consider to make this a reality.

1. Congress should mandate that the paper record is the legal record of the vote. The voter certifies this record accurately represents his or her selections before the vote is cast. The focus of the electronic voting machine is to assist the voter in creating a certified, paper record of the vote.

2. Electronic voting machines should also create an electronic record of the vote to be used efficient for tallies and tabulations.

3. The electronic record and the paper record should be linked with a unique identifier.

4. The voter should be issued a receipt indicating that he or she voted and be given the linking identifier to his or her voting record. The voter should be able to confirm that indeed his or her vote has been counted and has been audited while not being given access to the record details.

5. Paper records of the vote should be easily and accurately machine readable in order to provide efficient audits and validation.

6. Electronic voting machines and voting processes should be re-engineered to insure that all voting records are accounted for and human error is minimized.

7. As a check and balance, electronic voting system hardware and software should **not** be provided by a single vendor.

8. Electronic voting system hardware vendors must publicly disclose all internal and external interfaces of their systems.

9. All voting system software should be "open source" and available for public review.

10. Copyright and intellectual property protection should be available to rigorously protect voting systems software.

11. All existing electronic voting systems should be upgraded with software and systems that meet the above criteria. Congress should provide funds for this upgrade.

TruVote intends to provide software and voting systems which meet these requirements.

Thank your for the opportunity to present this information to you.

Larry W. Holmstrom

Verifiedvoting.org

October 3, 2006

Voter Verified Paper Ballots: Seat belts for Election Safety

Verified Voting's Testimony for the Committee on House Administration's hearings on Electronic voting machines: verification, security, and paper records

ABSTRACT

Secure, reliable, usable, accessible , and verifiable voting systems are critical to ensure accurate, transparent, fair, and inclusive elections. A number of states and local jurisdictions have deployed systems that meet all of these goals, but others have had substantial problems, particularly with Direct Recording Electronic (DRE) touchscreen systems. There is overwhelming evidence that currently-deployed DRE voting systems suffer from security vulnerabilities, reliability problems, and usability issues that put the integrity of our elections at risk and erode public confidence in election results. Procedural solutions that only address the physical security of voting machines are inadequate to protect against these risks.

As the experience of many states and local jurisdictions has demonstrated, the only effective voting solution available today is a system of voter-verified paper ballots (such as precinct-based optical scan voting systems combined with accessible ballot marking devices), that are used to conduct compulsory manual audits of electronic tabulations. Some touchscreen systems that produce individual ballots as well as accessibility for voters who are disabled or do not speak English have proven to be useful supplements to optical scan systems, but poorly-designed and crudely-built voter-verifiable paper audit trail (VVPAT) DRE printers that are unreliable have put requirements for voter-verified paper audit trails into question.

As a result of failures in paperless DRE voting technology, significant numbers of eligible voters have already been denied their right to vote, e.g., because they were turned away from their polling place because of inoperative voting machines. Failures in VVPAT technology have meant such machines failed to properly record votes that were correctly cast. As a result, some election results have been compromised due to such failures of DRE technology -- failures that could have been prevented had computer scientists' earlier warnings been heeded.

In light of the very serious security, reliability, usability, and verifiability problems with recently-deployed, HAVA-mandated voting systems that have become apparent during subsequent elections in a number of States, it is time for Congress to revisit HAVA and enact legislation to ensure that all voting systems enable eligible voters to cast their votes and have those votes counted in a manner that is secure, accurate, verifiable, accessible, and reliable. Any updates to HAVA must also ensure end-to-end transparency so that all aspects of the voting process are open to and observable by the public, from the testing and certification of machines through the final tabulation and canvass of the ballots. Voter confidence in our electoral process will only be restored if citizens are able to monitor and verify the process by which election results are reached.

Durable paper ballot records are like seat belts. We need to use them to prevent serious injuries to our democratic system when inevitable and sometimes serious incidents occur. Just as some early

seatbelt technology was awkward to use, the answer is not to throw out seat belt requirements, but rather to improve seat belt technology and legislation.

Most Voting Experts and Advocates Share Many Goals In Common

Although different voting experts, advocacy groups, and public officials differ on what voting equipment can best meet the our needs for accurate, reliable, secure, accessible, and transparent elections in the United States, most of us share a number of fundamental goals, including:

- *accuracy:* voting equipment should faithfully record and preserve the voting intentions of individual voters and minimize the numbers of votes lost;
- *verifiability*: all voters must have the opportunity to verify that their votes have been recorded correctly;
- *fairness:* voting equipment and procedures must not favor any particular candidate, party, or group nor exclude any eligible voters from casting a ballot;
- *reliability:* voting equipment and procedures must be sufficiently robust that breakdowns are rare, maintenance and upgrades relatively easy, and failures do not result in keeping voters from voting;
- *usability:* voting equipment must be easy for poll workers to set up and operate and for voters to use -- even poll workers and voters who are not experienced with computers;
- *accessibility:* voters should be able to vote independently and in private
- *trustworthiness:* voting equipment and procedures must be sufficiently transparent that both experts and the general public can have verifiable confidence that each stage of the election process has minimized the possibilities of fraud and error.

These are not mutually exclusive goals; they can be achieved through careful selection of voting technologies.

It has repeatedly been said that the States are the laboratories of our democracy. The last four years (i.e., from the enactment of the Help America Vote Act to the present) represent a national experiment in which thousands of jurisdictions have evaluated which voting technology will best achieve these goals. Now that most jurisdictions have completed that process, it is instructive to review the results from those "laboratories".

A Clear Majority: Optical Scan Paper Ballots

As a recent report from Election Data Services (EDS 2 Oct 2006) documents, many states and local jurisdictions have adopted new voting technology in the past four years since HAVA made federal funding available for that purpose. Lever, punch card, and paper-only systems have been almost completely replaced by optical scan and direct recording electronic (DRE) touchscreen equipment.

From November 2000 to November 2006, the EDS study estimates that the number of counties using Optical Scan equipment increased from 1,279 to 1,752 (41% to 56%), and the number of counties primarily using DRE technology) increased from 309 to 1,142 (10% to 37%). In terms of estimated registered voters, 84 million (49%) are in jurisdictions that will use optical scan technology and nearly 66 million (38%) are in jurisdictions that will use DREs in the November 2006 elections. (for the full report, see http://www.edssurvey.com/files/NR_VoteEquip_Nov-2006wTables.pdf)

Thus, a clear majority of jurisdictions have chosen to deploy optical scan paper ballot systems, and some states[1] have successfully used this technology for over 20 years. In addition, some states (e.g., Alabama, New Mexico and Michigan[2]) which had previously deployed DRE voting machines in some counties decided to retire those machines and convert to a precinct-count optical scan (PCOS) voting system statewide. And Connecticut, which had previously planned to replace its lever machines entirely with DREs has abandoned that plan and instead will deploy PCOS technology statewide.

These jurisdictions have realized that PCOS technology offers many advantages over DREs, including:

1. All voters use the same ballot, regardless of whether they vote absentee or in-precinct.
2. PCOS is scalable: only one scanner is needed per precinct regardless of number of voters, so long lines are rare.
3. Optical scan is a mature technology used reliably for over 20 years.
4. Optical scan paper ballots are inherently voter-verifiable and don't require VVPAT printers.
5. In the case of recounts or manual audits, optical scan paper ballots are much easier to hand-count than continuous-roll paper tapes printed by VVPAT printers attached to DREs.

A Clear Majority: Voter-Verified Paper Record[3] Requirements

There is widespread popular support for voter-verifiable paper ballots as the simplest, easiest, and most cost-effective way to maintain and improve the quality of our elections. To date, 28 states[4] have passed voter-verified paper record requirements, and another eight states[5] are deploying voter-verifiable equipment statewide, through their recent HAVA purchases. Thus 36 states (over 70%) have concluded that systems providing voter-verifiable paper records are necessary for trustworthy elections.

In addition, VVPR legislation has been introduced in several other states[6], and the legislatures of several pivotal states have come very close to enacting VVPR requirements recently.[7] That those bills have not yet passed has more to do with fiscal concerns or political maneuverings of a few powerful committee chairs.

Thirteen states have already explicitly required mandatory audits of the voter-verified paper records.[8]

---

[1] http://www.tulsaworld.com/OpinionStory.asp?ID=061001_Op_G6_Simpl24546

[2] http://www.michigan.gov/documents/Uniform_Voting_System_2_71047_7.pdf 2003

[3] It is important to note that voter-verified paper records (VVPR) are not limited to voter-verified paper audit trails (VVPAT) attached to direct recording electronic (DRE) voting machines. The broader term includes paper ballot-based systems such as the precinct-count optical scan used in more jurisdictions nationwide than any other system. Paper ballots, marked by the voter, are inherently voter-verified.

[4] Before 2000, NH and SD had statutes requiring paper ballots. IL, MI and NV passed voter-verified paper record requirements before the end of 2003. In 2004, AK, CA, ME, MO and OH added requirements, and NV became the first state to fully implement VVPAT with DREs. Details at:http://verifiedvoting.org/article.php?list=type&type=13#state.

[5] AL, MA, MS, ND, NE, OK, RI, WY

[6] Twelve states and the District of Columbia have introduced and/or are currently considering a VVPR requirement.

[7] E.g. Maryland, where this year such legislation passed unanimously in one chamber but was denied a meaningful hearing in the other, despite urging by the Governor; Iowa, where the bill passed unanimously in one chamber but was attached to un-passable language in the other; Tennessee, where a legislative study committee is set to review the matter; Virginia, where strong bi-partisan bills were tabled due to budget issues, but not rejected.

[8] http://verifiedvoting.org/downloads/ManualAudits-06-06.pdf

Several bills[9] in the U.S. House of Representatives would require voter-verified paper records (VVPR), of which H.R. 550 is the clear leader with 219 bi-partisan co-sponsors; it also provides the most comprehensive and effective solution. A majority of Members of the U.S. House of Representatives are on record as supporting this bill, while an even larger majority are on record as supporting legislation to enact a VVPR requirement for all voting systems used in federal elections.

Earlier this year, the US League of Women Voters passed a resolution in support of the use of voter-verifiable paper ballots/records for routine audits, and decrying the lack of a recountable audit trail in "paperless" electronic voting systems.[10] It is time for legislators and elections officials to discard the discredited assertion that non-voter-verifiable records (be they invisible electronic records or paper reprints of those records) are acceptable for audits of vote tallies from electronic voting systems.

DREs Without Independent Verification Are Inherently Insecure

Many flaws in the security design of DREs have been discovered over the last three years, as described below. However, these serious problems are all described in the context of *external* attacks, by people who do not have legitimate access to the voting machine internals.

It is crucial to note that there are many people with *legitimate* access to voting machine internals, who are capable of perpetrating "insider attacks," and that current technology allows no direct way to prevent or even detect such attacks by certifying the system design or software. ***The only feasible solution is to have an independent way of checking the results recorded by the machine.***

The only acceptable solution that is currently available and certified is a paper record of the vote that the voter can verify for correctness before the vote is cast. This enables an independent check, since the paper records can be manually counted and compared with the electronic results. If there is an error on the paper record, the voter can see it and report and correct it. If there is an error in the electronic record, it can be caught because it will disagree with the paper record.

There are a variety of other proposed methods for independent verification, including end-to-end cryptographic systems, audio-tape copies of the ballots, and photographs of computer screens. Most of these schemes are not currently available and certified. Those that are certified are too complex for voters and poll workers to understand, or have other gross deficiencies.

The possible existence of paperless independent verification in the future is neither a rationale nor an excuse for purchasing or using totally insecure and untrustworthy paperless technology now.

DRE Security Problems Have Been Documented Extensively

In contrast to optical scan technology, paperless DRE technology suffers from a number of severe problems, including security, usability, reliability, and trustworthiness. Over the past 3 years, a number of in-depth studies of voting system security have been published, and each one has

[9] http://www.verifiedvoting.org/legis
[10] http://www.verifiedvotingfoundation.org/article.php?id=6363

identified extremely serious security vulnerabilities involving paperless[11] electronic voting systems -- vulnerabilities that pose grave risks for our electoral system. These studies include:

1. "Analysis of an Electronic Voting System", Tadayoshi Kohno, Adam Stubblefield, and Avi Rubin, Johns Hopkins University and Dan Wallach, Rice University, July 2003.[12]
2. "Risk Assessment Report Diebold AccuVote-TS Voting System and Processes ", Science Applications International Corporation, September 2003. (An official report commissioned by the State of Maryland).[13]
3. "Direct Recording Electronic (DRE) Technical Security Assessment Report", Compuware Corporation, November 2003 (An official report commissioned by Ohio's Secretary of State)[14]
4. "Trusted Agent Report Diebold AccuVote-TS Voting System", RABA Innovative Solution Cell (RiSC), Dr. Michael A. Wertheimer[15] Director, January 2004. (An official report commissioned by the State of Maryland).[16]
5. "Federal Efforts to Improve Security and Reliability of Electronic Voting Systems Are Under Way, but Key Activities Need to Be Completed" (GAO-05-956)", GAO, October 2005.[17]
6. "Security Analysis of the Diebold AccuBasic Interpreter ", Dr. David Wagner, Dr. David Jefferson, Dr. Matt Bishop, California State Voting Systems Technology Assessment Advisory Board, February 2006. (An official report commissioned by the Secretary of State of California).[18]
7. "Diebold TSx Evaluation: Critical Security Issues with Diebold TSx", Dr. Harri Hursti, Black Box Voting, May 2006. [19]
8. "The Machinery of Democracy: Protecting Elections in an Electronic World", Lawrence Norden, et al.; Report of the Brennan Center's Task Force on Voting System Security, June 2006[20]
9. "Security Analysis of the Diebold AccuVote-TS Voting Machine", Ariel J. Feldman, J. Alex Halderman, and Dr. Edward W. Felten, Center for Information Technology Policy and Dept. of Computer Science, Princeton University, September 2006. [21]

Many of these reports, especially those published this year, address critical security concerns related to the use of removable memory cards in electronic voting machines. (While problems with these cards are not the only security problems identified in these reports, they are among the most serious.) These memory cards are routinely used to transfer information from one machine to another, much like floppy disks were used in the first generation of personal computers. Examples

---

[11] By "paperless electronic voting systems", we refer to those systems that do not produce a voter-verifiable paper ballot (VVPB) , hence systems that are "paper-less". While we acknowledge many existing DRE systems contain an internal printer used to print paper "zero tapes" prior to the opening of the polls and "summary tapes" once the polls are closed, we still refer to such machines as "paperless" unless such machines are also equipped with a printer that produces a VVPR. We use the term "paperless" rather than "VVPR-less" because it is more readable.

[12] https://www.eff.org/Activism/ E-voting/20030724_evote_research_report.pdf

[13] http://www.verifiedvoting.org/downloads/votingsystemreportfinal.pdf

[14] http://www.sos.state.oh.us/sos/hava/compuware112103.pdf

[15] Dr. Wertheimer now serves as the Assistant Deputy Director and Chief Technology Officer in the Office of the Deputy Director of National Intelligence: http://www.dni.gov/press_releases/20051031_release.htm,

[16] http://www.raba.com/press/TA_Report_AccuVote.pdf#search="raba report diebold".

[17] http://www.verifiedvoting.org/article.php?id=5826

[18] http://www.ss.ca.gov/elections/voting_systems/security_analysis_of_the_diebold_accubasic_interpreter.pdf

[19] http://www.blackboxvoting.org/BBVtsxstudy.pdf

[20] http://www.brennancenter.org/programs/downloads/Full%20Report.pdf

[21] http://itpolicy.princeton.edu/voting/ts-paper.pdf

of such usage include the authorized installation of certified software updates, the downloading of ballot formats for an upcoming election, or the uploading the votes cast by voters in an election that has just ended. Some of these operations are performed by poll workers, some by election officials, and others by technicians employed by the voting system vendor, presumably under the supervision of election officials.

In all of the recent reports , various modes of attack are described by which an adversary who obtains unauthorized access to a removable memory card located in an electronic voting machine can corrupt the vote tallies and voting records produced by that machine. The first few of these reports focused on the potential for such unauthorized access to occur either while a voting machine was at, or in transit to or from, the polling place for an election.

Vote-Stealing Code Can Be Spread By Virus-Infected Memory Cards

The seriousness of DRE security vulnerability was recently documented in a September 2006 publication of the security vulnerability study by the team of researchers at Princeton University led by Prof. Edward Felten. That study revealed (and demonstrated) a previously unexplored vulnerability posed by such removable memory cards: their ability to transmit a computer virus that spreads between voting machines and memory cards whenever the latter is plugged into the former. In this manner, a single infected card could introduce such a virus into a population of voting machines, many weeks or even months before an election. Over time, as unsuspecting elections officials moved memory cards between voting machines in the course of routine election activities (e.g., downloading ballot formats or uploading votes) , they could unknowingly spread the virus to more machines. As the Princeton team demonstrated, that virus could be used to introduce vote-stealing software onto all such infected machines.

This discovery by the Princeton team invalidates an oft-repeated assertion by voting system vendors and other proponents of paperless electronic voting machines: that such machines are immune to computer viruses because they are never connected to the Internet. Just as humans can be infected with viruses in multiple ways, so can computers -- and voting machines. Long before the Internet existed, computer viruses spread between early PC's via floppy disks moved from one machine to another, just as the removable memory cards are now moved between voting machines.

Thus, even if, for the sake of argument, one assumes that effective mitigation procedures can be implemented in practice to prevent (or at least detect) any tampering with the removable memory card in a voting machine while it is at (or in transit to or from) the polling place, that does not ensure that that memory card or voting machine was not already infected, long before it was configured and secured (i.e., tamper-evident tape applied) in preparation for shipment to the polling place. Even more insidious is the fact that the memory card and/or machine might have been unknowing infected by an honest election official or poll worker in the course of routine and fully-authorized election-related activities performed by those individuals. Once a machine is infected, that infection can only be detected or disinfected by means of a very labor-intensive process conducted by a relatively-skilled technician.

While the expert who identified the specific vulnerabilities described in the Princeton study was given access to that system to examine it (and justifiably so, given earlier revelations about poor security design in these systems), we have no way of knowing if or how many other persons with sufficient access (and ill intent) may have quietly uncovered these vulnerabilities earlier.

Currently, tens of thousands of such vulnerable machines are deployed nationwide, and many of them have been deployed since 2002, i.e., fully four years before the publication of the Princeton study and the concerns it has now raised about the risk of such infections. Thus, many of those machines were in circulation long before the mitigation procedures were issued by several states earlier this year. Accordingly, some of those machines may have been infected prior to the application of these mitigation procedures. Putting such mitigation procedures into effect at this late date may be about as effective a means of preventing infection as first starting to apply mosquito repellent several years after moving to a malaria-ridden region.

It is currently unknown what fraction of vulnerable DRE machines and memory cards may already be infected with viruses of the type demonstrated in the Princeton study, and answering that question would require a costly and time-consuming forensic examination of *all* such machines and memory cards currently in circulation, as well as disinfection of any machines or cards found to be infected. And unless such disinfection is complete across all machines in a jurisdiction (or until such DREs are re-engineered to provide immunity to such viruses), disinfected cards or machines could become re-infected if exposed to any card or machine that was still infected.

Unfortunately, most states have not ordered such examinations of their deployed DRE machines, either because they lack the resources to do so or they optimistically assume that no such infections have yet occurred. Based on the extensive spread of viruses throughout other forms of electronic technology (e.g., personal computers, cell phones, and even ATM machines[22]), it seems both risky and naive to assume that no such viruses are already circulating among DRE voting machines whose inherent design places that at very high risk to such viruses.

This problem cannot be solved in any practical sense by the application of tamper-evident tape or by applying, at this late date, strict chain of custody procedures for machines and memory cards which may already be infected. The only viable solution today is employ a system of voter-verified paper records that are checked via compulsory manual audits of those records.

Physical Chain of Custody Is Not Sufficient

In response to the alarm raised by those reports, a number of states (e.g., Ohio[23] and Florida[24]) issued advisory warnings recommending that local jurisdictions employ specific mitigation measures, including stricter procedures for monitoring the chain of custody for such voting systems as well as the use of serially-numbered tamper-evident tape to seal the access doors that cover the slots into which the removable memory cards are inserted. Some states, such as California, took stronger action, temporarily suspending or delaying certification of such voting systems and then certifying[25] those systems conditional on the strict application of such mitigation measures. Assuming that such measures could be counted on to prevent any unauthorized access to these vulnerable removable memory cards from occurring or going undetected, state election officials argued that these measures would be sufficient to eliminate the risks associated with these use of these cards.

---

[22] "Nachi worm infected Diebold ATMs", http://www.theregister.co.uk/2003/11/25/nachi_worm_infected_diebold_atms/

[23] http://www.sos.state.oh.us:80/sos/electionsvoter/advisories/2006/Adv2006-03.pdf

[24] http://election.dos.state.fl.us/pdf/memorandum.pdf

[25] http://www.ss.ca.gov/elections/voting_systems/cert_doc.pdf

Unfortunately, while such mitigation measures seem like they should be effective in theory, strict enforcement of such measures has so far proven to be very difficult for poll workers and elections officials to carry out in an actual election environment. For example, during recent elections (e.g., California's June 2006 primary election or Maryland's September 2006 primary) in jurisdictions where such mitigation measures were required (e.g., San Diego County, CA or Baltimore County, MD), the actual effectiveness of such measures has been questionable at best. Poll workers in those jurisdictions have reported numerous problems with the tamper-evident tape, including:

1. difficulty in determining when a tape has been tampered with, because the resulting change is appearance is hard to discern visually[26]
2. having inadequate training to know whether a legitimate piece of tape has been removed and replaced by a counterfeit piece.[27]

In addition, California's statewide requirement for maintaining a strict chain of custody for such electronic voting system conflicts with San Diego County's longstanding practice of sending such voting systems home with poll workers in the days or weeks preceding the election. As a result, such machines were left unattended and unsupervised for lengthy periods of time in poll workers' homes, garages, vehicles, or other potentially-insecure locations. Consequently, the state-imposed "chain of custody" requirement that was part of these mitigation measures was not strictly enforced, despite the fact that the State's certification of the voting system used in that county were conditional on the strict enforcement of that requirement.

Thus, these sorts of mitigation measures that only address the physical security of voting machines(either while they are located at the polling place or are in transit to or from that location) are difficult to implement in practice, given the performance of the tamper-evident tape currently in use, the skill and training level of poll workers, and the currently-funded methods for distributing massive numbers (e.g., 10,000) of voting machines to large numbers (e.g., 1,500) of polling places in counties such as San Diego, California. Accordingly, such mitigation measures are inadequate to address the previously-documented security risks associated with the use of these removable memory cards.

Although we entrust election procedures to our dedicated election officials and poll workers, we must ensure that the integrity of our elections never hinge on protocols so complex that they exceed their skills and training. And we must ensure that any mitigation procedures (implemented to address security vulnerabilities in voting systems) are not so fragile and intricate that they won't be strictly applied and enforced.

Certification Procedures Are Woefully Inadequate

It is important to be absolutely clear: the insecure paperless voting systems described here made it all the way through the existing federal certification process, despite the fact that these security vulnerabilities that were first mentioned in January 2004,[28] and recently expanded upon.[29] No certification system, even improved over today's systems, can catch all such vulnerabilities.

---

[26] http://avi-rubin.blogspot.com/2006/09/my-day-at-polls-maryland-primary-06.html
[27] http://cha.house.gov/hearings/Testimony.aspx?TID=1324
[28] http://www.raba.com/press/TA_Report_AccuVote.pdf
[29] http://www.ss.ca.gov/elections/voting_systems/security_analysis_of_the_diebold_accubasic_interpreter.pdf (California Secretary of State); and www.blackboxvoting.org

Nor will a certification system catch ballot programming errors, since such programming is unique for each election and thus does not go through the certification process. Ballot programming errors (not uncommon, and generally representing honest mistakes rather than sinister plots) pose a very significant risk to the accuracy and verifiability of elections conducted on paperless DREs. Tighter certification systems will do nothing to protect against such risks.

Paperless DRE Systems Are Neither Trustworthy Nor Fail-Safe

Simply put, existing paperless DREs cannot be made trustworthy. No paper trail printed post-election, without the benefit of voters confirming that the document represents their intent, can change that. Neither can the application of tamper-evident security tape. The suggestion that a reprint of unverifiable electronic ballot images, never reviewed nor confirmed accurate by the voters, can be used to conduct a meaningful audit has been soundly and repeatedly discredited.

Existing paperless DREs represent a *system* problem that cannot be resolved by *procedures*. Established organizations such as the Brennan Center have concluded that paperless DREs are *not* trustworthy[30], and the addition of VVPAT, audited to check machine tallies for accuracy, is the only way to *make* such systems trustworthy[31]. One must change the system itself: deploy an independent paper record of voter intent, confirmed by the voter, to use as the audit document and the true record of the vote.

Another critical function of voter-verified paper records, apart from security is that they provide a vital seat belt in case of accidents and other emergencies. VVPRs resolve the problems that occur when machine malfunctions result in lost electronic vote information.

A voter-verified paper record printer, for example, would have resolved the problem in Carteret County, NC in 2004 when 4400+ votes were irretrievably lost, affecting the outcome of a statewide race in which the margin was less than 2000.[32] After that unfortunate (and costly) event, NC passed a voter-verified paper record law. Each election, new examples arise – either of situations where votes were irretrievably lost, but could have been recovered if a VVPR requirement were in place, or of problems discovered and resolved because VVPR systems were in place.

A problem encountered with the scanner component of a paper ballot system need not result in lost votes. If the marked ballots are correctly managed, retained and recounted, votes can still be counted in a number of different ways. But a DRE which fails may lose these votes forever.

---

[30] U.S. GAO (see: http://www.verifiedvoting.org/article.php?id=5826), Johns Hopkins Institute, Raba Trusted Agent Report for MD's legislature and the Brennan Center's Task Force on Voting System Security: http://www.brennancenter.org/programs/downloads/Full%20Report.pdf

[31] Carter-Baker Commission (see http://www.verifiedvoting.org/article.php?id=5824), CA Voting Systems Technology Advisory Board, League of Women Voters (June 2006)

[32] http://www.wral.com/news/3891488/detail.html

[35] Testimony to the EAC from a Nevada election official regarding their initial implementation of VVPAT printers somewhat contradicts these concerns for one vendor's design; he said it was relatively simple, in the particular system they used, to change the printer cartridges and it could be done during the voting day with minimal interruption.

DREs Require More Extensive Secure Ballot Boxes

A fundamental distinction between DREs and paper-based systems that is often overlooked involves both the transparency and number of ballot boxes associated with each type of system. And this distinction has a profound effect on the level, complexity, and effectiveness of the procedures that elections officials and poll workers must employ to ensure the security of the ballot boxes.

In any voting system where ballots of record are paper (such as PCOS), each precinct has one (and only one) ballot box that is typically some sort of locked receptacle into which the optical scanner deposits the paper ballots after scanning them (or into which voters directly deposit their ballots in the case of a central-count optical scan or hand-counted paper ballot system). Security requirements for such ballot boxes are relatively simple. Prior to election day, the empty ballot box for each precinct requires no special security precautions because it not only contains nothing of value, it contains nothing at all.

On the morning of election day, at the opening of the polls, there is a simple and publicly-visible and verifiable process by which poll workers, along with the first voter of the day, can confirm that the ballot box really is empty: they can open the lid, look inside, feel the inside with their hands, or perform whatever other reasonable means of physical inspection they care to employ to verify that that ballot box really is empty. Once so verified, the lid is closed and locked in place, and the first voter of the day permitted to deposit his or her ballot. From that point on, until that ballot box is transported to the tabulation facility and unlocked, that ballot box is under the watchful eye of the all of the poll workers and observers at that polling place or at the tabulation facility. Once the canvass is completed, the ballot box is unlocked, emptied, and no longer requires that it be securely stored or access to it controlled and logged. Thus, each precinct requires only one such ballot box, and the security of that ballot box need only be monitored from the morning of election day until the completion of the canvass for that election.

In a DRE-based system, each precinct has at least as many ballot boxes as it has DREs, since the removable memory card in each machine each constitutes a separate, electronic ballot box. (In addition, each DRE has one or more redundant internal memories, each of which constitutes a "backup" electronic ballot box.) If the DREs and removable memory cards are always transported to and from the polling place as a sealed unit, then the number of distinct items for which "chain of custody logs" must be maintained is simply the number of DREs, whereas if they are transported in separate packages an even larger of items needs to be logged and tracked.

In addition, the security requirements for these electronic ballot boxes (both the removable memory cards and the DRE machines with their redundant internal memories) are much more extensive than those for the ballot boxes used for paper ballots. Each electronic ballot box must be subject to strict security protocols and chain of custody procedures at all times, even between elections. Otherwise, if there is a lapse in such procedures and a malicious individual obtains even brief access to either a removable memory card or a DRE machine, the potential for infection exists. Once such an infected memory card or machine enters the equipment pool in a given jurisdiction, elections and poll workers can unknowingly spread that virus as cards are moved between machines during routine operations that occur either during or in-between elections.

Unlike simple locked boxes that are used as ballot boxes for paper-based voting systems, poll workers and polling place observers have no direct method for verifying that any of the electronic

ballot boxes deployed at a given precinct are indeed empty (or uninfected) on the morning of election day. The only method they have is to ask the DRE to print out a "zero tape"; in other words, the poll workers and observers can't verify for themselves that the electronic box is empty, they have to ask the DRE and take its word. As Dr. Felten's demonstration illustrates in such a compelling way, if the DRE or its memory card is infected with a virus carrying a vote-stealing payload, then the "zero tape" printed by the DRE has little meaning. Further, some systems' software allows for the retroactive printing of a "zero tape" – well after voters have begun casting votes on the device – rendering it essentially meaningless.

In summary, systems which have a paper ballot of record impose a considerably lower security burden on elections officials and poll workers, because only one ballot box is needed per precinct, and it only needs to be secured from the start of the election until the end of the canvass for that election. In addition, it provides poll workers a direct and transparent means of verifying that the ballot box is empty at the start of the election. In contrast, a DRE system imposes a much higher security burden, because multiple (electronic) ballot boxes are needed per precinct and those need to be secured at all times. Furthermore, those electronic ballot boxes are opaque and poll workers have no direct means of verifying at the start of the election that they are either empty or uninfected.

Thermal Paper Rolls Are Not Adequate For VVPR

While many of the security and verifiability problems with DREs can be addressed by the addition of voter-verifiable paper record (also referred to as voter-verified paper audit trail, or VVPAT) printers, to date, the reliability and overall performance of such printers has been mixed. While elections officials from Nevada (the first state to deploy VVPAT printers) have testified to the EAC that such printers have performed well since their introduction in 2004, other jurisdictions, such as Cuyahoga County, Ohio, reported significant problems with their VVPAT printers during the primary elections of 2006. Accordingly, significantly better designs and operational procedures for such printers must be developed to address the serious reliability concerns that were raised in Cuyahoga County. In addition, printers that fail to perform reliably once deployed should have their certification suspended until such reliability problems are resolved.

In addition, VVPAT printers that print onto rolls of thermal paper present additional problems. First, they potentially compromise ballot secrecy, because votes are recorded onto the paper roll in the same order in which ballots are cast. Someone keeping track of the order in which specific voters cast their votes on particular machines could then deduce from such paper rolls how those voters had cast their votes. Second, in the case of a recount or manual audit, it is cumbersome and time-consuming for election officials to hand count votes recorded on such rolls of paper, especially given that such paper may be relatively thin and can potentially be damaged during the handling that would occur during such recounts or audits.

For all these reasons, such thermal roll paper VVPAT printers represent a poor method for enabling DRE voting machines to produce a voter-verified paper record. However, such printers represent just one possible method for providing a VVPR. Rather than fail to implement VVPR requirements because some of these types of printers were badly designed and have performed poorly, the proper solution is to either

improve the design of such printers or switch to a different technology for producing the VVPR.

It is instructive to compare the development of VVPAT printers to the evolution of seat belts in cars. Automobile vendors initially fought the requirement for seat belts: "they won't be effective, they will cost too much, most people won't use them," etc. The first generation of seat belts were not so effective, not comfortable to wear, and most people didn't use them. However, the public and the government rejected arguments that requirements for seat belts were a bad idea, or that the push for seat belts should be abandoned because of poor initial implementation. Requirements expanded, and vendors produced more effective and more comfortable seat belts. Information campaigns target those who forget to buckle up.

VVPAT/VVPR requirements are the seat belts for already-deployed voting systems, a necessary protection to ensure those systems are secure, accurate, reliable, and auditable. Some vendors have been resistant to put significant effort into this technology, and some first generation VVPAT systems may not be well-designed, reliable, or user friendly. It is no surprise that some election officials may find such systems difficult to deploy or that some voters may not verify the printouts from VVPAT printers.[35] Improved standards and public pressure will compel vendors to do a better job of implementation. And just as information that seat belts save lives caused many more drivers to actually use them, improved education about the crucial nature of the independent paper record will increase the public's scrutiny.

RECOMMENDATIONS

1. In order to address extremely serious voting system security vulnerabilities, a voter-verifiable paper record must be produced by all voting systems to enable voters to verify that their votes have been recorded properly.

2. Mandatory manual audits of the voter-verifiable paper records from a sample of precincts selected at random must be used to check the electronic tallies produced by voting systems. Without such audits, the VVPRs alone provide insufficient benefit.

3. Jurisdictions using DRE voting systems must implement a reliable means of providing VVPR, either by attaching *reliable* VVPAT printers to their DREs or by phasing out their DRE systems and converting to precinct-count optical scan systems (as Michigan did) augmented with accessible electronic ballot marking devices to ensure accessibility.

4. Any DRE+VVPAT system must have safety measures to maintain the consistency of the paper and electronic records, such as refusing to accept more electronic votes when the printer is not functioning properly.

5. In order to be certified for use, VVPAT printers must be highly reliable when set up and administered by average poll workers with average training

Submitted Testimony for The Hearing of The Committee on House Administration

Warren Stewart, Policy Director, VoteTrustUSA

September 18, 2006

VoteTrustUSA is a nonpartisan national network serving state and local election integrity organizations working to promote transparent, fair, observable, and audited elections. We advocate improved Federal and State standards for election processes and voting systems, improved testing and certification procedures for voting equipment, accurate and more complete reporting of election data, and a more widespread understanding of concerns about the accuracy, security, and reliability of all electronic voting systems. We advocate significant routine manual audits of voter-verified paper records of the ballots to check the operation of the electronic equipment. We support improved procedures for state and local election administration and poll worker training. We support the development and employment of voting systems that provide all voters both independent access to vote casting and confidence in the accuracy of vote counting.

We oppose the use of voting systems that do not provide an individual, permanent, voter verified paper record of each vote suitable for a meaningful hand-counted audit or recount. We oppose the involvement of voting machine vendors in the administration of elections, and we oppose any form of secrecy in the process of vote counting.

VoteTrustUSA applauds the Committee on House Administration for holding a hearing to address the issue of electronic voting security and verification and the decision to include a broad range of opinion on this critical subject.

In his opening statement Chairman Ehlers quoted H.L. Mencken, who wrote, "for every complex problem there is a solution that is clear, simple, and wrong." Without questioning the wisdom of Mencken's axiom, it could just as easily be observed that for every complex problem there is a solution that is opaque, complicated, and wrong.

As Prof. Simons noted in her testimony, a paper ballot optical scan voting system like that used in Chairman Ehlers' district, in Mr. Cunningham's county in Ohio, by a majority of jurisdictions across the country, and in almost every county for absentee voting, is the optimal currently available voting system. Optically scanned paper ballots, marked by the voter, are inherently voter verified, provide voters with notification of over- or undervotes, allow for efficient initial counts, but have the overwhelming advantage of providing the opportunity for humanly observable hand recounts and audits. Accessible optical scan ballots can be produced using tactile ballots or electronic ballot marking systems. Paper ballot optical scan systems have also proven to be significantly less expensive for jurisdiction to implement and maintain.

Voter Verified Paper Audit Trails, understood as printers attached to direct recording electronic voting machines, are a worthy attempt to address a fundamental flaw in those

machines: the fact that DREs do not provide an independent means of verification in the form of a contemporaneous record verified by the voter. As long as this fundamental shortcoming of DREs is left unaddressed, these machines will continue to meet with increasing resistance from the primary stakeholders in elections – voters.

The VVPAT printers currently produced by the leading vendors are inadequate and disappointing. That voting system standards have been adopted that have allowed such printers to be certified and implemented is also disappointing and should be corrected. Just as many of the witnesses argued that severe security vulnerabilities in currently available DRE voting systems should not lead to the abandonment of electronic voting entirely, so too, should clearly the flawed VVPAT printer attachments currently available lead to the abandonment of VVPAT printers. Rather, VVPAT printers should be rigorously tested to meet stringent reliability and usability before being entrusted to the critical function of ensuring the accuracy of vote tallies, just as the DREs themselves must be rigorously tested to meet stringent standards.

The increasing nationwide call for paper ballots should not be misinterpreted as a reactionary call for a return to punch cards as references to 'hanging chads' might suggest. It is also inaccurate to make the claim as one of the witnesses did that legislation that would require voting systems to produce or require the use of a voter verified paper record "would restore us to the year 1890, when anyone who wanted to tamper with an election needed to do no more than manipulate pieces of paper."

The witness also claimed that Rep. Holt's bill "the "Voter Confidence and Increased Accessibility Act" (HR 550) would "outlaw an entire category of voting machine with which we have a quarter-century of experience". As Mr. Holt pointed out HR 550 does not prohibit the use of DREs and it expressly allows the use of paper ballot optical scan voting systems – neither of which were available in 1890. Ignoring the numerous improvements in the administration of elections and the enhanced security procedures implemented by legislators and election officials across the country since the 19th century, it is disingenuous at best to make the claim that requiring an independent means of verifying the accuracy of votes counted by proprietary software, which has been demonstrated repeatedly to be prone to error, vulnerable to malicious attack, and inherently unobservable would return us to the 1890s.

While HR 550 was not the express subject of the Committee hearing, this bill, which has been co-sponsored by a majority of the members of the House, was never far from the surface and was directly attacked by one of the witnesses. Mr. Shamos claimed in his testimony that HR 550 was based on three major assumptions, all of which were false. First, he argued that HR 550 "assumes that paper records are more secure than electronic ones, a proposition that has repeatedly been shown to be wrong throughout history." He later explained that his claim derived from the bill's provision that in the case of discrepancies between manual counts of the voter verified paper record and electronic tallies the totals derived from the hand count shall be considered the "true and correct record of the voter's vote". Shamos claimed that HR 550 assumes that paper records are more secure than electronic ones and therefore "irrebuttably (sic) presumed to be

correct". He went on to discuss the ESI report, which found that many of the voter verified paper records were obviously flawed or nonexistent. As VoteTrustUSA has discussed earlier (see Appendix 1, "HR 550 and The Superiority of Paper Records"), HR 550 merely places the burden of proof on the party contending that the electronic totals were accurate. In the case of Cuyahoga County it would be quite easy to demonstrate that the paper records were inaccurate. The question, in the case of Cuyahoga, would be which of the irreconcilable electronic totals was accurate? The language of HR 550 could easily be clarified in mark-up if such clarification was even necessary legally.

Mr. Shamos' second "false assumptions" of HR 550 – that paperless touchscreens are auditable was not substantiated. If he was referring to the redundant memory provided by most DRE systems, his claim is meaningless, since not only did the various "redundant" memories examined in the ESI study conflict with each other, but the same error or attack that corrupted one memory would corrupt any redundant memory. The objective of a voter verified paper record is precisely that the voter can verify it and that it is independent of the electronic tabulation of the votes. While it may be theoretically possible to reconstruct the action of voters through the flash memory on some systems, this has never been attempted, presents privacy issues, is impractical, and has met with formidable resistance from election officials and vendors when it has been suggested.

The third "false assumption" was that "paper trails actually solve the problems exhibited by DRE machines". It is reassuring that Mr. Shamos has not been reluctant to admit that problems with DREs exist, but it must be pointed out that no one, including Mr. Holt, has asserted that "paper trails" would solve the problems exhibited by DRE machines. "Paper trails" especially as manifested in the extraordinarily flawed continuous roll, thermal paper printers that have been developed by the major voting machine manufacturers and certified by vendor-funded testing labs, are inadequate and emblematic of the extraordinarily poor quality of the products that have been purchased to count our votes.

Later Shamos baldly claimed, "The effect of HR 550 would be to ban electronic voting entirely in Federal elections." However, more than half the states already require have provisions very similar to HR 550, that require that voting systems produce or require the use of voter-verified paper records and their machines are not outlawed and will not be outlawed. What's more, almost half the polling places in America will use paper ballot systems in November and every absentee ballot will be a paper ballot, as both Dr. Simons and Rep. holt pointed out - paper ballots marked by voters are inherently voter verified.

Mr. Shamos also said that HR 550 "sets forth conditions that are not met by any DRE system currently on the market in the United States." However all the major vendors have developed voter verified paper audit trail printers to meet the demand of state laws that already exist in a majority of states. Mr. Shamos admitted as much in his next paragraph when he referred the "DRE paper trail systems that are currently on the market". As Mr. Holt pointed out later in the hearing, his legislation wouldn't outlaw any particular type of machines, only unverifiable ones.

Later Mr. Shamos made the unsubstantiated assertion that "the failure rate of paper trail DREs is double that of DREs without paper trails." It is unclear what methodology or source materials he was using as a basis for this statement, but in any case he is comparing apples and binary files. If a printer jams or runs out of ink, the problem and its solution are immediately apparent. There is simply no possible way of knowing how many times DREs have failed to accurately count votes.

Adding a specifically Pennsylvanian argument, Mr. Shamos claimed that HR 550 would violate statutory provisions in more than half the states that require a secret ballot. He claimed that the DRE paper trail systems currently on the market "either enables voters to sell their votes, or allows the government and the public to discover precisely how each voter in a jurisdiction has voted." It is unclear how a voter verified paper record retained in the voting booth and preserved according to the secure chain of custody procedures in effect in each state for paper ballots in general, as HR 550 requires, would allow a voter to sell his or her vote. I suppose a voter could take a camera with them and photograph the paper record, but then they could photograph the screen of the DRE as well. In the small number of jurisdictions in which voters sign in at the polling place rather than by signing an alphabetical voter roll, the currently available VVPAT printers that retain the paper records sequentially would allow someone with access to both the sign-in list and the VVPAT to determine how each voter voted – a legitimate concern. However, this could easily be overcome by requiring that the printers cut each paper record like every ATM machine does or by having voters sign alphabetically arranged voter lists.

Shamos next assured the committee that he is in favor of voter verification. He notes that "while [the voter verified paper record] shows the voter that her choices were properly understood and recorded by the machine, it offers no assurance whatsoever that her ballot was counted, that it will ever be counted, or that it will even be present when a recount is conducted. Once the polls have closed, the voter not only has no recourse or remedy, but is powerless to even determine whether her vote is part of the final tally or to object if she believes it isn't." Of course this is true with or without paper and its much worse without a paper record. In the case of a DRE with no independent means of verification, there is absolutely no reason that any voter should have any confidence whatsoever that her vote is being counted correctly and absolutely no recourse whatsoever to object if it isn't.

In conclusion, VoteTrustUSA strongly recommends the use of paper based optical scan voting systems, with ballot marking devices to provide disabled voters with the opportunity to vote privately and independently. If direct recording electronic voting systems are to be used, they should provide an independent means of verification in the form of a contemporaneous permanent record that can be verified by the voter in the voting booth before the vote is cast electronically and that is preserved according to established procedures and regulations for paper ballots in general. Voters should not be required to trust voting systems that do not provide a transparent, observable, and independent means of counting their votes.

Appendix

HR 550 and the Superiority of Voter Verified Paper Records
By Warren Stewart, VoteTrustUSA
April 14, 2006

Andrew Gumbel's recent book "Steal This Vote" provides a detailed and discouraging survey of how the integrity of election results have been compromised and manipulated since the beginnings of the grand experiment in representative democracy was launched after the American Revolution. It hasn't mattered what voting system was being used – paper ballots, lever machines, punch cards, or touchscreens – the political advantage to be gained from criminally altering election results will always pose a temptation for fraud.

Given the rich history of election fraud accomplished through the manipulation of paper ballots, the provision calling for the superiority of voter verified paper records in the case of discrepancies found in legislation like HR 550 has been called into question. What if someone managed to tamper with the voter verified paper records, whether they are optically scanned paper ballots, or simultaneous records generated by printer attached to a DRE? In the event of fraud or manipulation of the paper record, would HR 550 require that corrupted totals derived from paper records would nevertheless take precedence over electronic tabulation?

A reading of the language of HR 550 relieves these concerns.

Section 2(a)(2)(B)(iii) of HR 550 reads "in the event of any inconsistencies or irregularities between any electronic records and the individual permanent paper records, the individual permanent paper records shall be the true and correct record of the votes cast." Section 2(a)(B)(i) of the same bill requires that the voter verified paper records be preserved "in a manner which is consistent with the manner employed by the jurisdiction for preserving paper ballots in general." Thus all of a state's procedures and requirements for securing the chain of custody of those records would apply.

In the event of a discrepancy, one party will seek to defend the electronic tally, and the other will seek to defend the paper tally. Under the language in the bill, the burden of proof will be on the party seeking to defend the electronic tally to prove that the paper tally has been compromised in order to negate the bill's presumption of the preemptive validity of the paper records over the electronic tallies. That can be demonstrated vastly more readily (by way of witness testimony pertaining to breaches on the chain of custody of the paper records, a simple count of the available records as compared to the number of voters who signed in, and so on) than the reverse as there is no evidence as to the accuracy or inaccuracy of the electronic tally other than the voter verified paper records).

Because the voter verified paper records are the only ones verified by the voters, rather than by the machines, and because those records are the only evidence available by which to confirm or challenge the accuracy of the electronic tally, they must be considered the vote of record. This assumes, of course, that it is the actual voter verified records that are

being used in the comparison. The party seeking to defend the electronic tally need only prove that it is not the actual voter verified paper records that are being used (by presenting such evidence as is noted above, e.g. that the ballot box was switched, or stuffed, etc.) in order to render void the bill's special blessing given to the actual voter verified paper records.

That is how the language reads and how it would have to be interpreted by any reasonable judge, since the entire purpose of the bill is to create an independent audit record in order to check the machine count. All that said, it would be a simple matter in the process of a mark-up to request the addition of a clarifying sentence that said something like "in the event of a discrepancy the voter verified paper records shall be considered the vote of record and the burden of proof shall be on the party seeking to defend the electronic tally to demonstrate by compelling evidence that the set of voter verified paper records being used in the audit or recount have been tampered with and upon such proof, the contest shall be subject to a re-vote.

OFFICE OF THE STATE'S ATTORNEY
COOK COUNTY, ILLINOIS

RICHARD A. DEVINE
STATE'S ATTORNEY

Public Interest Bureau
69 W. Washington - Suite 930
Chicago, IL 60602
312-603-8600

To: Interested Persons

From: Kelly Pierce, Disability Specialist

Date: October 4, 2006

I have become aware of widespread citation of my March 2005 accessibility review of four voting machines that were being considered for purchase by Cook County and the City of Chicago Board of Election Commissioners. Since this report was written, meaningful and substantial accessibility improvements have occurred. Following the public demonstration of the four voting machines on March 15, 2005, Cook County Clerk David Orr announced on May 26, 2005 that he had chosen Sequoia Voting Systems as the new election system for suburban Cook County. The next week, the Chicago Board of Elections followed with a similar announcement. The first electronic voting machine to be used would be the AVC Edge. On June 13, 2005, Sequoia Voting Systems then President and CEO Tracey Graham met with disability leaders and the Cook County Clerk and described the company's substantial commitment to improving the accessibility of the AVC Edge. An audio recording of a voting experience was produced that day following this meeting. The recording and end user experiences with the Sequoia AVC Edge were used to produce a June 30, 2005 report on the audio interface of the machine. Since completion of the report, Sequoia representatives spent more than 100 hours in enhancing and improving the audio script used by the AVC Edge, states a December 2005 memorandum by Sequoia President Jack Blaine. More than 20 hours were spent with city and county officials and leaders from the disability community reviewing the effectiveness of each audio prompt on the machine. Further, Sequoia redesigned its control box for the audio interface. The new control unit included easy to locate volume control buttons and a switch that increased or decreased the rate of speech in the audio recording. The new control unit also enabled those who could not use their hands to vote to plug in a sip and puff device so the ballot could be voted completely from someone's assistive technology.

Additionally, Sequoia committed to numerous other changes for the November 2006 election. In September 2006, Sequoia representatives met with the Cook County Clerk, the Executive Director of the Chicago Board of Election Commissioners and leaders in the disability community to demonstrate the new and enhanced accessibility features of the Sequoia Edge II Plus voting machine, which will be used in the November 2006 election. The Sequoia Edge II Plus replaces the AVC Edge used in the March primary election. The audio interface now includes navigational prompts on the contest menu and an interactive ballot review mode so blind and disabled voters can exit the review mode at a particular contest and change their selection as sighted voters can. The now accessible ballot review will largely resolve the problems that were described in my report by a Santa Clara County, California blind voter. The experiences of this voter, which were quoted in the report, were shared recently in testimony before a congressional committee. The company may refine the accessibility of its ballot review, further increasing the accessibility and usability of this newly accessible function. The re-designed touch screen on the Edge II Plus has legs that can be adjusted to different levels for various wheelchair heights. For the first time, people who have low vision will be able to view the ballot using a zoom function which magnifies the type up to 400 percent its normal size as well as view the ballot at a high color contrast. Sequoia has re-designed its audio control unit yet again. The buttons are concave and recessed so those with head or mouth sticks and pointing devices can operate the machine independently. There are now also separate large plug-in "buddy buttons" for people with limited dexterity to use. More substantial enhancements to the accessibility of the Sequoia Edge II Plus are planned in time for the municipal elections in spring 2007.

At that time, most, if not all, of the accessibility problems identified in March 2006 will be dramatically reduced if not eliminated altogether. The flexible nature of information technology as deployed as electronic voting machines made the accessibility changes and enhancements possible. As has been stated in multiple reports by the National Council on Disability, a federal agency, when representatives of industry, government, and the disability community work together cooperatively as partners in using technology to solve accessibility problems, the inconceivable becomes possible enabling a new level of independence never before achieved.

The Only Independent Voting and Vote-Verification Method for People who are Deaf-Blind

Vote-PAD
Patent Pending
Vote-PAD, Inc.
660 Jefferson Ave.
Port Ludlow, WA 98365

How are folks who are deaf-blind supposed to be able to vote privately and independently?

To the best of our knowledge, the Vote-PAD is currently the only voting system that truly gives completely independent and private access to voting for voters who are deaf-blind.

The Vote-PAD is a very simple assistive device that lets you mark and verify your votes on a standard paper ballot and to do it privately, by yourself.

The heart of the Vote-PAD is a plastic ballot sleeve, into which a paper ballot is slid. There are holes in the plastic sleeve that line up with every position you might want to mark on the ballot, and there are large tactile identifying bumps next to each of these marking holes. A separate Braille guide booklet explains which holes are for which candidate or choice on the ballot. Hearing folks can use an audio guide tape, instead of Braille, if they prefer. You use a standard pencil or pen to mark in the holes for each of your choices.

When you are done marking your votes, you can then verify your marked choices with the verification wand. This wand works somewhat like a vibrating light probe. You just place the tip into the hole you think you marked, and press the button. It will vibrate if it senses a good pencil or pen mark.

For voters who want to write in a name of an unlisted candidate, the tactile ballot sleeve has cut out windows for the write-in boxes. For voters who can't do hand writing in these write-in windows, there are separate tactile write-in grid sheets. These tactile write-in sheets have columns of alphabetized raised-line boxes that can be marked with a pencil or pen. This lets you spell out your write-in candidate's name, by just moving across the columns and marking a letter box in each of the columns.

The Vote-PAD binder that holds the one or more tactile ballot sleeves has front and back covers to keep your ballot hidden until you are ready to slide your paper ballots out of the sleeves and into the ballot box, privately and independently.

Because the Vote-PAD is so simple, compact, and inexpensive, you could even use it from home, to vote absentee, without having to go to a polling place. What other voting system would allow folks with disabilities to privately and independently vote absentee, from their own home?

Would it be fair to deny deaf-blind voters the use of an available system that can let them vote privately and independently? Obviously not! It is important that deaf-blind folks and others concerned about voting rights make sure that their election officials know about the availability and need for accessible voting assistive devices like the Vote-PAD.

Ellen Theisen
President, Vote-PAD, Inc.
www.Vote-PAD.us

AFFIDAVIT OF NOEL RUNYAN

Noel Runyan, being duly sworn and upon his oath, states:

1. [redacted]. I give this affidavit to assist the court in determining whether the Sequoia AVC Edge Direct Recording Electronic ("DRE") touchscreen voting machine meets the disability access requirements of the Help America Vote Act of 2002 (HAVA). In my opinion, as an expert in the field of disability access and as a disabled (blind) person, the AVC Edge DRE falls far short of meeting those requirements. I explain this opinion in more detail below.

2. The basis for my opinion is my over thirty-six years of experience with microprocessors, digital logic, analog circuits, speech output, human interface design, and development of access technology for persons with disabilities, including extensive development and application of speech and braille interface technologies. My opinion is also based on my own experience, as a blind voter, voting in actual elections on the Sequoia AVC Edge DRE voting machine.

3. I received a BS in Electrical Engineering and Computer Science from the University of New Mexico in May 1973. I was named the Eta Kappa Nu Most Outstanding Electrical Engineering Student in the United States for 1972. In 1971, I received the Engineering Open House Sweepstakes Award for my project, "Digital Voltmeter with Braille Output". Also in 1971, I was awarded 1st place Local, 3rd place Regional prizes in the Institute of Electrical and Electronic Engineers (IEEE) Paper Contest, "Aids and Devices for the Visually Handicapped Engineer".

4. While a student, in 1968-1969, I worked at the Air Force Weapons Lab,



Kirtland AFB on programs for simulating atomic bomb blasts. In 1970, I worked on Mapsis, a tactile graphics program, at the University of Kansas.

5. From 1973 through 1978, I was employed by IBM. My projects included design and testing of magnetic stripe card security systems testing the security for ATMs and for Bay Area Rapid Transit system (BART) ticket machines, nonvisual display technology research, systems architecture, electronic logic design, and human factors engineering. At IBM, I developed the first text to speech program ever used on microprocessors. I used speech synthesizers and microprocessors to develop advanced prototype devices for the visually impaired. I co-invented the first talking touch screen/tablet system. I received an IBM Special Contribution Award in 1978.

6. From 1978 through 1983, I was employed by Telesensory Systems. My projects included development of a serial interface, and other portions of the original VersaBraille, the first braille laptop computer. I developed and patented a vibrating dots Braille display system. I was in charge of the Voice Output Communications Aid (VOCA) research and development project and the TeleBraille deaf blind communicator research and development project.

7. In 1983, I founded a company, now known as Personal Data Systems, to develop communications systems for persons with visual impairments. I headed up the hardware and software design and the development of the Audapter Speech synthesizer and the Talking Tablet System. I authored the EasyScan, BuckScan and PicTac scanning software programs. I helped design accessible touch screen information kiosks. Recently, I have been involved in the development of talking medical

devices and accessible talking internet radio systems.

8. I have extensive experience in integrating computer systems with speech, braille, and large print output. I also have experience with the array of adaptive technologies for persons with manual dexterity handicaps, gained while I was the principal investigator on a National Science Foundation funded research project for developing voice output communications aids (VOCAs) for folks with motor impairments. Many people with problems like Cerebral Palsy cannot speak with their own voice and cannot use a standard keyboard to type messages. As part of this project, I had to become familiar with alternative data input and control systems for people with various keyboard impairments. These alternatives included head mounted laser pointers, foot switch, eye gaze, eye blink, and puff-and-sip switch scanned input systems (in which the user blows or sucks air to control a communications device) and other systems. In addition, I worked with Telesensory Systems' alternative lap tray communications product called the Autocom, an electronic lap tray communications system that used a magnetic selector puck, instead of a keyboard.

9. The New Mexico Election Code requires that all voting systems "shall meet federal election standards" to be approved for use in New Mexico. NMSA 1-9-2(A). The current iteration of the federal standards appears, in part, in the Help America Vote Act ("HAVA"), which requires that all voting systems used in elections for federal office anywhere in the United states shall "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." HAVA § 301(a)(3)(A), 42 U.S.C. § 15481(a)(3)(A). According to the federal Election Assistance Commission (EAC), established by HAVA, "[c]ompliance with Section 301(a)(3) requires that the voting system be accessible to persons with disabilities as defined by the Americans with Disabilities Act, including physical, visual, and cognitive disabilities, such that the disabled individual can privately and independently receive instruction, make selections, and cast a ballot." EAC Advisory 2005-004, issued July 20, 2005. This means, among other things, that states acquire and make available to disabled persons voting machines that will accommodate the basic range of disabilities, including such as Cerebral Palsy, aphasia, low vision, blind, deaf blind, and home/institution bound. The Sequoia AVC Edge voting system accommodates none of these disabilities adequately.

10. I am thoroughly familiar with the disability access capabilities of the Sequoia AVC Edge DRE voting machine, having reviewed the manufacturer's specifications, attended vendor demonstrations, and having cast my vote on the Sequoia voting machines in several actual elections. In my opinion, the Sequoia AVC Edge DRE does not satisfy the disability access requirements of HAVA, as incorporated into New Mexico law. This opinion is based on (1) the Edge's complete lack of any accommodation for persons with severe physical dexterity impairments who are unable to use touchscreens or keypads; (2) the gross inadequacy of the Edge's audio assist feature for persons who are blind or low vision; and (3) the Edge's failure to accommodate elderly voters who have developed severe visual impairments with age but are unfamiliar with and unable to cope with audio-only access technology because

they have had normal vision most of their lives. In short, it is my opinion that a large portion of disabled citizens who attempt to cast their votes on Sequoia AVC Edge voting machines will be unable to do so. Below, I will explain each of the deficiencies identified above.

11. As stated above, in order for a voting system to comport with federal requirements, a voting machine's adaptive technology must accommodate not only blind and low vision persons but also persons with physical disabilities, such as dexterity disabilities. Currently available adaptive technologies for persons with various keyboard impairments and complete inability to use hand controls, which are readily adaptable to voting machines, are head mounted laser pointers, foot switch, eye gaze, eye blink, puff-and-sip switch scanned input systems and electronic lap tray systems. The only practical way to connect these adaptive devices to a computer or other equipment the user wishes to control and operate, such as a voting machine, is through an electronic user interface connector. The Sequoia AVC Edge DRE voting machine has no support for these standard 2-switch systems or other user interface devices. Therefore, voters whose dexterity disability requires them to use head mounted laser pointers, foot switches, eye gaze, eye blink, puff-and-sip switch scanned input systems or electronic lap trays are not afforded "the same opportunity for access and participation (including privacy and independence) as for other voters" on the Sequoia AVC Edge DRE, nor can a voter with such a physical disability "privately and independently receive instruction, make selections, and cast a ballot."

12. The Sequoia Edge, from my direct experience, has no more than a poorly

functioning and ineffective audio interface and can only achieve magnification through external lenses. In my opinion, this falls far short of meeting HAVA standards. First, for voters who are low vision but not blind, the Edge does not provide the combination of touchscreen display modification capabilities necessary to accommodate the range of vision impairments. Vision impairments vary considerably from person to person. An adequate display modification system permits the user to change contrast, foreground and background colors, fonts and font size, with options for multiple font sizes or for zoom magnification. Enhanced display technologies for low vision users have been available for over 16 years and it should be easy to add this capability to computerized voting machines. As other DRE manufacturers have managed it, there appears to be no good reason that the manufacturer of these voting machines could not have easily adapted the Edge to provide accessible display technology.

13. For voters who are blind, voting machines must have an audio access feature that permits the blind voter to receive instructions and ballot choices and to make selections and cast their ballot nonvisually. The audio assist feature on the Edge is very poorly designed, complicated, and unacceptably tedious. My own experience voting on the Sequoia AVC Edge DRE with the audio assist feature in the November 2004 election illustrates the problems. After signing in, and getting my voter smart card, I had to wait 8 minutes for officials to manage to reboot the audio voting machine. The polling officers had been using it for touch screen voting, as there was a very long line and just 5 voting machines for our combined 2-precinct polling place. I had my braille notes in a hard-back notebook, so I could read my notes with the notebook on my lap.

The volume control on the front of the Edge key pad was not working well and resulted in scratchy and intermittent sound. By the time I got the volume set to where I could understand it, the introduction message had already finished the English instructions and was off into other languages. I was not sure what I should do, so I finally gave up and pressed the select button. This eventually got me to the language menu, where I was able to select English and get started with my ballot. I must emphasize that, in my opinion, my ability to navigate this process at all was due to my familiarity with computers and computer technology. I doubt that most blind voters would have been able to navigate it at all.

14. The first major problem I had was that the ballot on the Edge voting machine was not in the same order as the printed sample ballot. When my wife pointed this out to the chief poll worker, they were surprised to see the difference, and said maybe that would explain why they found that it was taking voters longer than expected to vote. Because my notes were done in the order of the sample ballot, I had to do a lot of hopping around in my notes and be very thorough and careful listening to the machine. In contrast to what we had been told, the list of candidate names was spoken in alphabetical order.

15. It took me thirty minutes to work my way through the ballot and make my selections. After that, I had quite a bit of trouble getting into the review mode, to get a full list of all my selections. When I did, it went on and on, for 23 minutes, like a long uncontrolled drink from a fire hose. The review function read each item, and then, at the very end, said what my selection was for that item. It even threw in the details of what

the fiscal impact would be, and took forever. This is completely backwards. It should announce the name of the item, then state my selection, and then read the rest of the information for that item. Also, I should have the control to press the arrow key to move forward or backward through the items, without having to listen to all the text about every item. When I did find that I had made a mistake in my selections, I had to wait until the end of the whole review process to correct it, instead of being able to stop, make the change, and then continue with the review where I left off. I did not want to abort the ballot verification review, to make a correction, and then have to start the 23 minute review all over again. When I later attempted to change one of my selections from "no" to "yes", the machine would not let me just select "yes", until I had first gone to the "no" entry and deselected it. This was very awkward and confusing. Again, I doubt that many blind voters would be able to navigate this process.

16. At one point, as I was nearing the end of the ballot, I was dumped back into the language selection menu. I was being very careful to not push the "help" button, so I don't know why this language menu popped up. For a scary minute, I was afraid I had just lost my ballot and was having to start all over. I re-selected "English" and fortunately was returned to my previous location in the ballot.

17. An additional frustration was that the volume on some of the messages was so much lower than the rest of the messages that I had to fiddle with turning up the volume, repeating the message, and then turning the volume back down before proceeding. The volume on all the messages should be normalized to make them the same. This is easy to do and should be done for all messages.

18. From the time I signed in and got my voter smart card, it took 8 minutes to reboot the machine as an audio voting machine, 30 minutes to make my choices, 23 minutes to review and verify, and another 4 minutes to make a correction and record my vote. Not counting the hour I had waited in line, it took me about 65 minutes to mark and record my ballot. It would have taken even longer if I had been willing to wait, as prompted, until the end of each message to push the "select" button. The messages misled some folks because they say something like, "...at the end of this message, you can press the ...". This implies that you are supposed to wait until the speech message finishes.

19. As an expert in the design of audio access technology, it is my opinion that the Edge system was incompetently designed. Additionally, as one familiar with the technology, I was far more likely than the average blind voter to be able to figure out how the Edge audio assist feature worked and was structured, yet I had considerable difficulty that slowed the voting process. Many blind voters might be embarrassed to tie up a voting machine for over an hour, or not have sufficient patience, and therefore decide not to vote the entire ballot or not to fully review their selections before casting the ballot. What I have heard from other voters, even sighted voters, is that they have often caught ballot marking mistakes in the review process. It is clear from this and from my own experience, that we really have to go through the review process in order to make sure that our ballots are accurate. The Sequoia review process is totally unacceptable and would cause most voters with disabilities to skip the review.

20. When I was finally done voting, I took a portable radio out of my pocket

and turned it on, with its earphone in my ear. The Sequoia Edge voting machine was broadcasting a lot of radio noise on the AM band. This RF noise emission represents a possible electronic eavesdropping threat to voting privacy. Also, I noted that none of the poll workers seemed to notice or ask what kind of electronic device I was using and for what purpose. From the standpoint of the security of the voting machines against electronic eavesdropping or hacking, the poll workers seemed to be too lax about letting people use cell phones, palmtops, or other electronic equipment in the polling place. There should have been, but were not, any announcements (audible or visible) warning voters against using cell phones, cameras, palmtops, or other electronic devices in the polling place.

21. There were at least two times when I wanted to ask for help from the poll workers. One was during the confusion I encountered from the difference between the printed sample ballot and the DRE ballot. The other time was near the end of my ballot marking, when I had a lot of trouble getting the review started and then was trying to find and change a mistake I found during the review. Unfortunately, the Sequoia Edge does not allow for simultaneous use of the audio assist feature and display on the touchscreen. Because the poll workers would not be able to look at a visual display on my system, and didn't have any way to join me in listening to the audio output of the machine, I assumed that I couldn't get much help from a poll worker (even though our head polling officer seemed very knowledgeable and helpful).

22. Finally, the Sequoia Edge does not address the needs of elderly voters who have developed severe visual impairments with age but are unfamiliar with and

unable to operate audio-only access technology because they have had normal vision most of their lives. This represents a large and growing portion of the voting population. Such persons are so accustomed to using their eyesight that they have extreme difficulty in understanding and using audio-only access alternatives to touchscreens or other visible ballots. For these voters, neither a fully adjustable touchscreen display nor the audio assist alternative is sufficient. Rather, they require the simultaneous use of both accommodations in order to vote independently and privately. In this configuration, the user can receive some information and cues visually and other information and cues audibly, and through the combination be enabled to vote without assistance. The Sequoia Edge voting machine does not permit simultaneous use of the touchscreen display and the audio assist feature. For similar reasons, it is unreasonable to expect people who may have no visual impairment but are motor impaired to use only the Edge's keypad and voice interface to operate the system.

23. In summary, it is my opinion that the Sequoia AVC Edge voting system is disability accessible in name only and is not a voting system that meets HAVA disability accommodation requirements in any significant respect.

I swear and attest under penalty of perjury under the laws of the State of New Mexico that the foregoing is true and correct. Executed this 19th day of December, 2005 in Campbell, California.

Noel Runyan

Noel Runyan

[NOTARY]

KAREN ARMSTRONG
COMM. #1578921
NOTARY PUBLIC - CALIFORNIA
SANTA CLARA COUNTY
My Comm. Expires June 12, 2009

State of California County of Santa Clara
Subscribed and sworn to (or affirmed)
Before me on this 19 day of December 2005 by
Noel Runyan
personally known to me or proved to me on
the basis of satisfactory evidence to be the
person(s) who appeared before me.
Signature
(Seal)

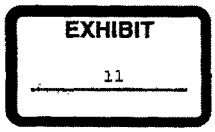
DISTRICT COURT, DENVER COUNTY, STATE OF COLORADO City and County Building 1437 Bannock Street Denver, Colorado 80204	
Plaintiffs: MYRIAH SULLIVAN CONROY *et al.* **Defendants:** GINNETTE DENNIS *et al.*	▲ **COURT USE ONLY** ▲ Case Number: 06CV6072 Div: 1 Ctrm: 1
Attorneys for Plaintiffs: Paul F. Hultin (Atty. Reg. #0142) Andrew C.S. Efaw (Atty. Reg. #29053) Michael T. Williams (Atty. Reg. #33172) Andrew H. Myers (Atty. Reg. #34288) Ramona L. Lampley (Atty. Reg. #37288) Wheeler Trigg Kennedy LLP 1801 California Street, Suite 3600 Denver, CO 80202 Telephone: (303) 244-1800 Facsimile: (303) 244-1879 E-mail: hultin@wtklaw.com; efaw@wtklaw.com; williams@wtklaw.com; myers@wtklaw.com; lampley@wtklaw.com	

DECLARATION OF NOEL HOWARD RUNYAN

I, Noel Howard Runyan, hereby declare:

QUALIFICATIONS AND SUMMARY OF OPINIONS

1. I reside at 638 Sobrato Lane, Campbell, California. I have been asked by counsel for Plaintiffs in this action to provide my opinion whether the Diebold Election Systems, Inc. ("Diebold") AccuVote-TSx ("Diebold TSx") Direct Recording Electronic ("DRE"), Sequoia Voting Systems, Inc. ("Sequoia") AVC Edge II DRE ("Sequoia Edge II"), and Election Systems and Software, Inc. ("ES&S") iVotronic Touch Screen DRE ("ES&S iVotronic") voting systems are 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. This Declaration also describes my personal knowledge and experience with DRE voting systems as a voter who is blind.



2. It is my opinion that the Diebold TSx, Sequoia Edge II, and ES&S iVotronic voting systems are not accessible for individuals with disabilities for several reasons, including:

a. Diebold TSx's, Sequoia Edge II's, and ES&S iVotronic's complete lack of a dual-switch capability without which the systems are inaccessible to voters with severe manual dexterity disabilities who are unable to use touch screens or keypads;

b. The inadequacy of the Diebold TSx, Sequoia Edge II, and ES&S iVotronic audio access features for persons who are blind, low vision, dyslexic, cognitively impaired, or severely motor impaired;

c. The three systems' lack of simultaneous and synchronized audio and visual outputs without which the systems are inaccessible for many voters with visual impairments (*e.g.*, the failure of the Diebold TSx, Sequoia Edge II, and ES&S iVotronic DREs to accommodate elderly voters who have developed severe visual impairments with age but are unfamiliar with, and unable to cope with, audio-only access technology because they have had normal vision most of their lives);

d. The verified voter paper audit trails ("VVPATs") on the three systems are inaccessible to many voters with visual or motor impairments, so that persons with disabilities cannot personally verify the printout of VVPAT printers on the Diebold TSx, Sequoia Edge II, and ES&S iVotronic systems;

e. All three systems' blatant lack of adequate privacy curtains to prevent eavesdroppers from reading the text of ballots on the visual displays of the DRE systems;

f. The three systems' lack of technology that allows voters with disabilities to select for themselves different modes or features to provide accessibility without intervention from poll workers; and

g. The Diebold TSx's, Sequoia Edge II's, and ES&S iVotronic's confusing menu selection systems that are difficult for people with cognitive disabilities to use effectively.

3. The above failures and omissions could have been corrected using existing adaptive or other available technologies.

4. My opinions are based on more than 36 years of personal and professional experience with microprocessors, digital logic, analog circuits, speech output, human interface design, and development of access technology for persons with disabilities, including extensive development and application of speech, Braille, and large print interface technologies. A copy of my curriculum vitae is attached (Plaintiffs' Appendix Exhibit 36). My opinions are also based on my professional experience with hands-on examination, testing, demonstration, and use of various voting systems, including the Sequoia Edge and Edge II, ES&S AutoMark, VotePad, and Diebold TSx voting systems, and two separate hands-on trials of the ES&S iVotronic voting system, as well as my personal experiences voting on the Sequoia Edge II machines in several real elections. My opinions

are also based on my review of current literature on voting system accessibility, technical specifications and publications of DRE system manufacturers, and other information gathered over the years at conferences, seminars, and workshops on accessibility issues. I have submitted expert witness declarations in other cases in Arizona, California, New Jersey, New Mexico, and Pennsylvania concerning access by individuals with disabilities to DRE voting machines. I testified as an expert witness at a preliminary injunction hearing in the Pennsylvania action.

5. I received a BS in Electrical Engineering and Computer Science from the University of New Mexico in May 1973. I was named the Eta Kappa Nu Most Outstanding Electrical Engineering Student in the United States for 1972. In 1971, I received the Engineering Open House Sweepstakes Award for my project, "Digital Voltmeter with Braille Output." Also in 1971, I was awarded 1st place Local, 3rd place Regional prizes in the Institute of Electrical and Electronic Engineers (IEEE) Paper Contest, "Aids and Devices for the Visually Handicapped Engineer."

6. While a student, in 1968-1969, I worked at the Air Force Weapons Lab, Kirtland AFB on programs for simulating atomic bomb blasts. In 1970, I worked on Mapsis, a tactile graphics program, at the University of Kansas.

7. From 1973 through 1978, I was employed by IBM. My projects included design and testing of magnetic stripe card security systems, testing the security for ATMs and for Bay Area Rapid Transit system (BART) ticket machines, nonvisual display technology research, systems architecture, electronic logic design, and human factors engineering. At IBM, I developed the first text to speech program ever used on microprocessors. I used speech synthesizers and microprocessors to develop advanced prototype devices for the visually impaired. I co-invented the first talking touch screen/tablet system. I received an IBM Special Contribution Award in 1978.

8. From 1978 through 1983, I was employed by Telesensory Systems. My projects there included development of a serial interface, and other portions of the original VersaBraille, the first Braille laptop computer. I developed and patented a vibrating dots Braille display system. I was in charge of the Voice Output Communications Aid (VOCA) research and development projects and the TeleBraille deaf blind communicator research and development projects.

9. In 1983, I founded a company, now known as Personal Data Systems, to develop communications systems for persons with visual impairments. I headed up the hardware and software design and the development of the Audapter Speech synthesizer and the Talking Tablet System. I authored the EasyScan, BuckScan and PicTac scanning software programs. I helped design accessible touch screen information kiosks. Recently, I have been involved in the development of talking medical devices and accessible talking Internet radio systems.

10. I have extensive experience integrating over 500 computer systems with speech, Braille, and large-print output. I also have experience with the array of adaptive technologies for persons with manual dexterity handicaps, gained while I was the principal investigator on a National Science Foundation funded research project for developing VOCAs for persons with motor impairments. Many people with problems like Cerebral Palsy cannot speak with their own voice and cannot use a standard keyboard to type messages. As part of this project, I had to become familiar

with alternative data input and control systems for people with various keyboard impairments. These alternatives included head mounted laser pointers, foot switch, eye gaze, eye blink, and puff-and-sip switch scanned input systems (in which the user blows or sucks air to control a communications device) and other systems. In addition, I worked with Telesensory Systems' alternative lap tray communications product called the Autocom, an electronic lap tray communications system that used a magnetic selector puck, instead of a keyboard.

METHODOLOGY, ANALYSIS, AND OPINIONS

11. The Help America Vote Act of 2002 ("HAVA") requires that all polling places in elections for federal office anywhere in the United States have at least one voting system that shall "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." HAVA § 301(a)(3)(A), 42 U.S.C. § 15481(a)(3)(A). I understand that Colorado's statutes incorporate HAVA's requirements regarding disability access for voting systems. According to the federal Election Assistance Commission (EAC), established by HAVA, "[c]ompliance with Section 301(a)(3) requires that the voting system be accessible to persons with disabilities as defined by the Americans with Disabilities Act, including physical, visual, and cognitive disabilities, such that the disabled individual can privately and independently receive instruction, make selections, and cast a ballot." EAC Advisory 2005-004, issued July 20, 2005. This means, among other things, that States must acquire and make available to disabled persons voting systems that will accommodate the basic range of disabilities, including such as Cerebral Palsy, aphasia, low vision, blind, deaf blind, and hearing impaired.[1] The Diebold TSx, Sequoia Edge II, and ES&S iVotronic voting systems do not accommodate these disabilities adequately.

[1] Cognitive impairments are impairments that make it more difficult for a voter to process information. For example, voters who have suffered strokes will often suffer some degree of cognitive impairment. Voters with cognitive impairments often will require accommodations that allow them to receive information about the ballot in more than one form simultaneously—for example, visually and through spoken messages.

Affordable Disability-Access Technologies Are Readily Available

12. Omission of proper access capabilities from the Diebold TSx, Sequoia Edge II, and ES&S iVotronic DRE voting systems cannot be attributed to impracticality of undue cost or unavailable technology. Adding the necessary switch-control inputs, alternative tactile-key controls, speech output, and easy-to-read large-text display to electronic voting equipment does not have to entail major costs or great technology breakthroughs.

13. For over 15 years, computer hardware and software have been successfully assisting persons with a wide variety of disabilities to meaningfully communicate with and use computerized systems. Although not perfected and not implemented evenly across all possible applications, computerized access technologies have made most computer systems reasonably accessible for most persons with disabilities. This is especially true in the case of access to personal computers.

14. Many blind or low vision folks can now regularly use large-text, speech, or Braille interface systems on computers to do word processing, email, and web browsing.

15. For over a decade, most personal computers have been able to speak to their users in a high quality voice, using only inexpensive software programs and the standard built-in hardware of the computer. Single-line Braille displays (although costing several thousand dollars or more) have been used by many blind computer users for decades.

16. For over 16 years, the standard built-in video hardware of personal computers has been powerful enough to allow screen magnifier programs to magnify screen text and images, adjust contrast, and customize the colors used for screen text and background.

17. For at least a decade, motor-impaired persons with some keyboarding capabilities have been typing on their personal computers, with the aid of software programs that adjust keyboard timing to prevent unwanted key presses or stuttering repeats. This type of keyboard access software also offers "sticky key" options to allow single-finger or mouth-stick entry of keystrokes that would normally require typing with two hands or multiple fingers.

18. For decades, there have been alternative input-control systems that allow severely motor impaired persons to input text and control computers with just a couple of special switches (like foot switches, large "jelly" switches, sip-and-puff switches, head-movement switches, and eye-blink switches). Sip-and-puff devices are devices that attach to the voting machine and allow the voter to indicate his or her choices by sipping air from or puffing air into a tube. Jelly switches accommodate voting for dexterity-impaired voters. Jelly switches are large buttons that are easier for a person with limited hand strength and dexterity to press. Most of these switch input systems use the standard 1/8-inch audio phone plug for their common interface. Head-mounted laser pointers, eye-gaze input systems, lap-tray puck-sensor systems, and voice-recognition systems are just a few of the many alternative input and control systems in common use for decades.

19. Today, many folks have sophisticated computerized wheelchairs with built-in accessible communications systems that allow their users to send text messages and send control signals to other computer systems.

20. To aid folks with hearing impairments, properly designed personal computer systems have, for many years, been able to route warning beeps through their sound systems and to redundantly indicate audible warning sounds, prompts, and messages with visual flashes, captions, or other visible cues.

21. This is not to say that all computer systems are completely accessible by all persons with disabilities. Rather, it is to demonstrate that many good, inexpensive, and mature access technologies have long been well known and readily available for computerized equipment designers to use in the design of equipment such as accessible electronic voting systems.

22. Other voting systems incorporate many of the standard access technologies, listed above, either singly or in combination. For example, the Hart InterCivic eSlate DRE and ES&S AutoMark ballot-marking machine both allow alternative input controls with switched devices, and the AutoMark and VotePad tactile ballot systems produce printed paper ballots that can be accessibly verified by voters with disabilities.

Missing and Inadequate Access Features on the Diebold TSx, Sequoia Edge II, and ES&S iVotronic DREs

23. I am thoroughly familiar with the disability access capabilities of the Diebold TSx, Sequoia Edge II, and ES&S iVotronic DRE voting machines, having reviewed the manufacturers' specifications, attended vendor demonstrations, having personally tested the Diebold TSx in a demonstration ballot-marking environment, having personally tested the Sequoia Edge II by voting on it in several real elections, and having performed two separate hands-on trials of the ES&S iVotronic voting system.

24. My own hands-on experiences with DRE systems manufactured by these vendors include the following:

- 2002 demonstration of Diebold AccuVote-TS DRE (the predecessor to the Diebold TSx) in a League of Women Voters ("LWV") booth, at a conference for the blind;
- 2003 evaluation of Diebold AccuVote-TS, ES&S iVotronic, and Sequoia Edge with mock ballots at the Peninsula Center for the Blind and Visually Impaired, Palo Alto, California;
- 2003 trial voting on Diebold AccuVote-TS in LWV booth at a conference for the blind;
- 2004 trial with mock ballot on the Diebold TSx at the American Council of the Blind summer conference;

- 2004 and 2006 voting four different times on Sequoia Edge II in Santa Clara County, California, elections; and

- April 2006 personal testing of the Diebold TSx and the ES&S iVotronic at the National Federation of the Blind Technology Center in Baltimore, Maryland.

25. I have also discussed, at length, the Diebold TSx, Sequoia Edge II, and ES&S iVotronic machines' designs and performances with several experts on accessible electronic voting systems, who also have personally tested the Diebold TSx, Sequoia Edge II, and ES&S iVotronic DREs with their audio access systems.

26. In addition to studying the VerifiedVoting.org and Electronic Frontier Foundation (EFF) descriptions of the features and operation of the Diebold TSx, Sequoia Edge II, and ES&S iVotronic, I have studied their specifications, features, and demonstration materials on the manufacturers' web sites. These included detailed step-by-step descriptions of how to vote both with and without their audio systems.

27. My personal and professional background, my hands-on experiences, my review of the manufacturers' and others' materials, and my discussions with expert users render me able to assess whether or not the Diebold TSx, Sequoia Edge II, and ES&S iVotronic are able to accommodate voters with disabilities. In my opinion, none of these three DRE systems satisfies the disability access requirements of HAVA and Colorado State law.

28. In short, it is my opinion that a large portion of Colorado citizens having disabilities and who attempt to cast their votes on Diebold TSx, Sequoia Edge II, or ES&S iVotronic voting machines will be unable to do so privately and independently. Below, I will explain each of the deficiencies identified above.

The Subject DREs' Failure to Accommodate Severe Dexterity Disabilities

29. As stated above, in order for a voting system to comport with federal requirements, a voting machine's adaptive technology must accommodate not only blind and low vision persons but also persons with physical disabilities, such as dexterity disabilities, as well as persons with hearing impairments, or cognitive disabilities.

30. There currently exist available adaptive technologies for persons with various keyboard impairments and complete inability to use hand controls, and these technologies are readily adaptable to voting machines. Such technologies include head switches, foot switches, giant jelly switches, and sip-and-puff switches. The only practical way to connect these adaptive devices to a computer or other equipment the user wishes to control and operate, such as a voting machine, is through a standard 1/8-inch phone-plug dual-switch interface. Diebold TSx, Sequoia Edge II, and ES&S DRE voting machines do not support these standard two-switch systems. Voters with manual dexterity disabilities who use a sip-and-puff switch, a foot switch, a head switch, or any other dual-switch adaptive device cannot plug that device into the Diebold TSx, Sequoia Edge II, or ES&S iVotronic to gain control over the system. Voters with manual dexterity disabilities who are unable

to use these three voting systems' manual selection buttons or touch screen are thus prevented from casting a vote using these voting systems. These defects deny voters with severe manual dexterity disabilities the same opportunity for access and participation (including privacy and independence) enjoyed by other voters who use these three voting systems.

31. Dual-switch adaptive technology has been available for more than 15 years, is affordable, and is easy to implement. The failure of the Diebold TSx, Sequoia Edge II, and ES&S iVotronic voting systems to include dual-switch adaptive technology is inexcusable and makes the systems inaccessible to most people with severe manual dexterity disabilities.

32. The sip-and-puff option proposed for the Sequoia Edge II would work only with audio output, and without visual display. It would force voters with severe motor impairments to vote as though they were also totally blind. Because Sequoia's sip-and-puff switch controls would only give voters the "Forward" and "Select" control input functions, they would not have access to the "Help" functions and would not be able to back up to hear something again or make corrections. Additionally, the audio orientation instructions and prompts are for using the tactile keypad and are totally inappropriate for two-switch users. This attempt to offer a sip-and-puff interface is bogus and not what the access industry would normally consider to be a two-switch or sip-and-puff interface. Normally, a two-switch interface to a system with a visual display would permit the user to select items on the visual display, instead of forcing them to use an exclusively audio output system built for blind users. Sequoia's proposed interface is token and represents a poorly considered, tacked-on approach to accessible voting system design. It will not functionally meet the needs of most of the severely motor impaired voters.

33. The Diebold TSx, Sequoia Edge II, and ES&S iVotronic DRE voting machines also do not support computerized communicators such as head-mounted laser pointers, eye gaze, eye blink, and electronic lap-tray puck-selector systems because they do not support serial or other standard I/O interfaces. Therefore, voters whose dexterity disability requires them to use adaptive technologies are not afforded "the same opportunity for access and participation (including privacy and independence) as for other voters" on these three voting systems, nor can a voter with such a physical disability "privately and independently receive instruction, make selections, and cast a ballot."

Inadequate Keypads

34. As specified in section 508 of the Americans with Disabilities Act (ADA): "Controls and keys shall be operable with one hand . . . ." Many voters with motor impairments cannot hold the Diebold TSx, Sequoia Edge II, or ES&S iVotronic tethered keypads in one hand, while attempting to press keys with the other.

35. Unlike smaller and more ergonomically designed single-hand-operated remote controls for television sets, the large size and form factor of the Sequoia Edge II and Diebold TSx keypads do not facilitate their use as a keypad held in a single hand and operated by the thumbs of the same hand.

36. Although Diebold's own literature represents the TSx's tethered keypad as a "tactile keypad," their telephone keypad with a bump on the 5 key is not what the access industry considers a tactile keypad. Its keys are much too small and too close together for most persons with major motor impairments to be able to use it. There are too many keys, including keys that have no function at all. Proper accessible keypads should have only a few keys and the keys should be much larger and be spaced further apart. Additionally, the keys should have high-contrast coloring, large print labels, and unique tactile shapes; all chosen to make them simple to discover, to identify intuitively, to remember easily, and to locate quickly.

37. The Sequoia Edge II tethered keypad is so big and bulky that many voters, not to mention those with dexterity impairments, find it very awkward to hold and operate, even with both hands.

38. Because the Sequoia Edge II has no built-in keypad cradle or place to park the keypad without being held by the voter, a standing voter is forced to try to hold the keypad in one hand and operate it with the other.

39. There is no place to leave the Sequoia Edge II keypad when you are through voting. I have personally found Sequoia Edge II voting machines in polling places with the keypads and earphones left hanging over the edge, by their cables, and dragging on the floor.

40. The Braille labels on the keys of the Sequoia Edge II keypad are difficult to read. They do not have the Braille dots spaced properly, with the standard Braille dot spacing. They are also so close to the back edge of the keys that it is difficult for many Braille readers to get their finger tips onto the dots to feel them.

41. The volume control slide pot on all of the Sequoia Edge II systems I've tried are of poor quality, noisy and scratchy, and there is no tactile indication for where it should be set for normal operation. Consequently, I missed the initial instruction message of the system before I figured out how to get the volume set properly.

42. The ES&S iVotronic does not even have a built-in volume control.

43. The Sequoia Edge II keypad has no speech rate control. Similarly, the ES&S iVotronic lacks a "speed control" over the audio output. This is important for the elderly and people with learning disabilities, cognitive disabilities or special needs who need to listen to the instructions and ballot selections at a slower rate than the fixed, default rate set by the system, while other voters cannot stand to listen to tediously slow speech. Voice speed control is standard adaptive technology that has been around for many years. It can be easily implemented, and commonly has been implemented, in computer systems, including electronic voting systems.

44. The data cable on the back of the Sequoia Edge II is so flimsily attached that the cable has to be secured to the back of the keypad by a tie wrap. This was clearly designed with the wrong type of connector plug.

45. The challenge of using such keypads or touch screens, for many folks with motor impairments, may be better appreciated if you imagine yourself trying to operate the touch screens, the keypad of the Sequoia Edge II, or the telephone-style keypad of the Diebold TSx with the heel of your hand, your elbow, a rod held in your armpit, or a small baseball bat held in your mouth. Instead of the small, indistinct, closely spaced keys on the Diebold TSx's telephone-style keypad, other voting devices such as the ES&S AutoMark have large, widely spaced, and distinct tactile keys.

46. The ES&S iVotronic also needs, but does not have, a detachable keypad that can be positioned on the lap, hand, or other convenient place if required. If designed properly, this adaptive tactile keypad technology, which has also been around for a long time, would allow more voters with motor impairments or reaching impairments to operate the input controls.

47. The proper operation of the system by the voter should be highly discoverable. This means that a voter should be able to figure out how to use the system without previous training and without significant instruction by a poll worker. To aid in this discovery, the Diebold TSx, Sequoia Edge II, and ES&S iVotronic should have audio key describer features, such as holding the Help key down while pressing a second key to produce a message describing the second key's function.

48. Additionally, the Diebold TSx, Sequoia Edge II, and ES&S iVotronic each need, but do not have, practice modes with a simplified example mini ballot, to give the voter who needs it a comfortable opportunity to figure out how to view, mark, review, and correct their choices.

49. The Diebold TSx, Sequoia Edge II, and ES&S iVotronic also do not have a "Call for Help" key or other control to discretely summon assistance from a poll worker.

50. As demonstrated in the Trace Center (Madison) proposal for an ideal voting system, the Diebold TSx, Sequoia Edge II, and ES&S iVotronic should (but do not) have an 1/8 inch phone jack (separate from the headphone jack) on the keypad, for attaching a sip-and-puff or other standard switched input-control device.

Inadequate Audio Interfaces for Blind and Low Vision Voters

51. The Diebold TSx, Sequoia Edge II, and ES&S iVotronic, from my direct experience, have no more than poorly functioning and ineffective audio interfaces.

52. The designs of the Diebold TSx, Sequoia Edge II, and ES&S iVotronic DREs require poll workers to enable the audio function for the voter. The selection of this access option and others, such as larger or smaller text size, should be available at all times, for selection by the voters themselves. Choosing to use access features should not require poll worker intervention such as reprogramming of the voter identification card (as is required by the Diebold TSx system), nor rebooting the system (as is required by the Sequoia Edge II). The current state of adaptive technology allows for people with visual disabilities to do "discovery" and "personal adaptation" on well-designed computer systems without intervention (*i.e.*, the ability to go to a computer system and immediately begin to privately adapt it for personal use). Just as voters can select a language choice on these systems by themselves, they should be able to select audio mode or video viewing enhancements by themselves, without the intervention of poll workers or third parties. There is no good reason that voting systems could not have personal configuration abilities for selecting access media.

53. The absence of this technology to allow immediate use and adaptation by people with disabilities without third party intervention causes several problems for people with visual and other disabilities. One is the total lack of privacy, as the voter is required to inform election officials in front of other people of his or her disability and the need for assistance, denying that voter privacy and independence. This problem is particularly acute for people who prefer to keep secret the fact that they have visual or reading impairments or other special needs.

54. Another problem with running the system in a completely separate audio mode is the possibility that the system will malfunction when it operates in a separate, special audio mode. In one well-publicized demonstration to California voting officials, a Sequoia voting system misrepresented votes when it was switched to Spanish language mode. A similar problem could occur when the ES&S iVotronic is switched to a special audio mode.

55. Voting with audio output on the Diebold TSx, Sequoia Edge II, and ES&S iVotronic is an excessively slow and tedious process. In the case of the Diebold TSx, this is due, in large part, to its annoyingly long, pregnant pauses between phrases or messages. It also has overly verbose prompts that relentlessly keep repeating unnecessarily long messages throughout the ballot marking process. However, when you need it to talk, the Diebold TSx audio prompting does not tell you how to return to reviewing the ballot.

56. Moving back and forth between reviewing and making changes in the Diebold TSx ballot can be a long, slow process, because it usually requires many repeated pressings of the forward or backup keys.

57. Many voters using the Diebold TSx, Sequoia Edge II, or ES&S iVotronic audio access feature would not be able to navigate their cognitively difficult hierarchical menus and ballot marking, review, and correction systems.

58. For example, the ES&S iVotronic voting system uses a complicated and confusing process for navigating its hierarchical menu system. Its poorly worded messages and complicated logic make it difficult to use, especially for the elderly and people with learning disabilities or cognitive impairments. A good example is that one button (the green, diamond-shaped button) is used on some screens to select a candidate but used elsewhere to move to the next race. A voting system with good human factors design would not have more than one function per button, to avoid confusion and erroneous voting. The navigation buttons also can cause confusion about what race you're on and who you're voting for. For example, initially, the voter is placed in the top level, or contest level, of the hierarchy, and uses the yellow "Up and Down" arrow buttons to move from contest to contest, and presses the green "Select" button to enter a race. Once in a particular race, the voter is at the bottom, or candidate level, of the hierarchy and again uses the "Up and Down" buttons to move from candidate to candidate. The voter presses the "Select" button to choose the candidate of his or her choice within that race. The problem is that if a voter moves past the last candidate in a race, the system immediately moves back up a level in the hierarchy to the contest level, positioned on the next race. If the voter realizes that he or she has been automatically moved out of one race into another race, they would have to move back to the original race they were working on and again press the Select button to move back down into the candidate level. If the voter doesn't comprehend what has happened in these situations (as is likely with the elderly or people with learning disabilities, cognitive impairments, dyslexia, or other special needs), the voter may be confused and think that he or she is selecting a candidate for one race while the system has actually moved on to another race.

59. In my opinion, this confusing system of input controls and multilevel menu system renders the ES&S iVotronic inaccessible to people with certain visual or cognitive impairments. This overwhelmingly complicated system will also cause some people with disabilities to skip voting altogether, or to "short circuit" the process, such as skipping the summary page. Incredibly, reading the summary page is the only way for a voter to confirm if they have "under-voted" (*i.e.*, failed to vote for enough candidates for every race).

60. An additional frustration I encountered with the speech on the Diebold TSx, Sequoia Edge II, and ES&S iVotronic DREs was that the volume on some of the messages was so much lower than the rest of the messages that I had to turn up the volume, repeat the message, and then turn the volume back down before proceeding. The volume on all the messages should be normalized to make them the same. This is easy to do and should be done for all messages.

61. To support the needs of audio voters who have major hearing loss, a high volume boost capability should be but is not available for Diebold TSx, Sequoia Edge II, or ES&S iVotronic machines.

62. When using audio output, the voter should always be able to turn off or on the visual display output. This would allow audio-only voters to have better privacy, if they want it, while

allowing them to re-enable the visual display whenever they desire. For example, it might be helpful for the voter to enable the visual display when asking for assistance from a sighted poll worker. Neither the Sequoia Edge II nor the ES&S iVotronic have a control to enable the video display while using the audio-voting feature.

63. If you are forced to stand while voting with either the Diebold TSx or Sequoia Edge II, you will need to detach the keypad from the side of the DRE and hold it in your hand.

64. As a Braille reader, I have found it extremely difficult to read the Braille notes I bring to the polling place, while trying to also hold and operate a keypad. When reading Braille, it is important to be able to keep one's place by keeping one hand on the Braille text. Having to switch back and forth between reading Braille and holding the keypad is tedious and time consuming, especially on long ballots. A lot of time is wasted each time I switch from holding the keypad to finding my place again in my Braille notes. The Sequoia Edge II has no cradle or other place to park its keypad for single-handed operation. This makes it very awkward and difficult to read Braille notes while using these keypads.

65. Unlike the keys of the Diebold TSx keypad, keys that are used to move forward or backward in an audio ballot should have shapes that indicate direction. For example, arrow-shaped keys that intuitively indicate their direction through the ballot choices.

Failure to Accommodate Voters Who Require Both Visual and Audio Access

66. The Sequoia Edge II and ES&S iVotronic systems do not allow for simultaneous and synchronized audio and video outputs. In other words, if these systems are in audio mode, the visual displays are disabled, and if the systems are in visual mode, the audio mode is disabled. This failure to allow simultaneous and synchronized audio and visual outputs makes the systems inaccessible for voters with visual impairments who require or prefer to have audio assistance when viewing the video display of ballot selections. This problem is particularly acute for elderly voters who have developed severe visual impairments with age but are unfamiliar with, and unable to cope with, audio-only access technology because they have previously had good enough eyesight for most of their lives. For these voters, neither a fully adjustable touch-screen display nor the audio access alternative is sufficient by itself. Rather, they require the simultaneous use of both audio and video display systems in order to vote independently and privately.

67. Empirical studies have confirmed that multi-sensory outputs are more accessible to voters with disabilities than single-sensory outputs. Indeed, these studies have shown that multi-sensory output systems reduce error rates for all voters. Adaptive technology that allows for such multi-sensory outputs has been around for many years, is affordable, and is easily implemented into computer systems. There is no good reason for the Sequoia Edge II and ES&S iVotronic voting systems to lack such basic access technology.

68. Proper operation of simultaneous audio/visual access does not mean just having the audio/keypad and video/touch screen working at the same time, as separate systems. Rather, it means that they must be integrated in a synchronous fashion. In a synchronous audio/visual output

system, selecting an item on the touch screen highlights it visually and also synchronously speaks it through the audio output.

69. Similarly, selecting an item with the keypad or switch input control alternatives should cause the item to be both spoken and visually highlighted.

70. Synchronized redundant input controls and output media allow the voter to play to their own strengths by focusing on the combination of controls and output that best fits their personal abilities.

71. Synchronized audio and visual display would also be valuable when the audio voter needs some assistance from a poll worker (assuming the voter has the ability to easily turn the visual display mode on and off and gets audible acknowledgement of the display mode).

72. For similar reasons, it is unreasonable to expect people who may have no visual impairment but are severely motor impaired to be able or willing to use only audio output to read and mark their ballot on the Diebold TSx, Sequoia Edge II, or ES&S iVotronic DRE machines.

73. The Diebold TSx, Sequoia Edge II, and ES&S iVotronic voting machines do not permit voters with disabilities to select their audio and visual display modes by themselves. Instead, they must get a poll worker to assist them by selecting the audio or visual modes for them. This requires that the disabled voter is aware of, and knows how to ask for, the proper audio/visual mode, and requires that the poll workers know how to properly select the synchronized mode for the voter. Synchronized audio/visual access mode should b the default access mode for all electronic voting systems.

74. In practice, the lack of technical training and expertise of poll workers has meant that many visually impaired voters have not been aware of the audio/visual access mode or have been unable to get their poll workers to set up their Diebold TSx, Sequoia Edge II, or ES&S iVotronic voting system properly to use it. For example, Karyn Campbell, in an article she sent to the American Council of the Blind Discussion List and other groups, described her first experience voting with a Diebold TSx machine in the Illinois March 2006 primary. She explained that she asked for an audio ballot, and had to have poll workers reprogram her voter ID card, as it did not set up the Diebold TSx properly the first time she tried it. When she put the reprogrammed card in the Diebold TSx machine, it started working in audio mode, but with the video output in the wrong mode. Not wanting to push her luck, she gave up and went ahead and voted with the Diebold TSx machine not configured as she needed.

75. In my own first voting experience with the Sequoia Edge II, the poll-workers were never able to get the DRE working in audio mode, even after 45 minutes of reading manuals and calling voter tech support service centers.

76. Because low vision voters would like to use large, clear text on the screen and may have difficulty detecting eavesdroppers, the lack of a privacy surround curtain enclosing the booth area (not just token privacy side panels), appears to be a serious or even totally unacceptable privacy breach. The side privacy panels of the Diebold TSx, Sequoia Edge II, and ES&S iVotronic systems

are inadequate for assuring privacy for all voters. The lack of a privacy curtain adequately enclosing the booth area creates an unacceptable privacy exposure.

77. The access functions of the Diebold TSx, Sequoia Edge II, and ES&S iVotronic systems are also not suitable for providing accessible voting to voters who are both profoundly hearing impaired and visually impaired. The lack of a standard output interface port means that, for example, a deaf-blind voter cannot bring his or her own portable Braille display device to the polls and plug it into a standard output plug of the DRE, in order to read the instruction materials, mark, review, and correct his or her ballot privately and independently.

78. In order to provide accessibility for people with hearing impairments, these DRE systems should have a "boosted" high volume capability for audio voters who normally need the higher volume levels of assisted listening. The absence of such a "boosted" volume setting on these DRE systems means that the systems are inaccessible for some audio-using voters with severe hearing impairments.

79. For voters who are low vision but not blind, the Diebold TSx, Sequoia Edge II, and ES&S iVotronic do not provide the combination of touch-screen display modification capabilities necessary to accommodate the range of vision impairments. Vision impairments vary considerably from person to person. An adequate display modification system permits the user to change contrast, foreground and background colors, fonts and font size, with options for multiple font sizes or for zoom magnification.

80. The Sequoia Edge II and ES&S iVotronic are not accessible for some people with astigmatism, color blindness, or other visual impairments because they do not provide for contrast control or foreground/background color selection. Contrast control allows for adjustment of the display's contrast sharpness (*i.e.*, high, medium, or low) while color selection allows a person to change from the default "black text on a white background" display to "white text on a black background" or some other color combination. Some visually impaired people prefer and need different colors or contrasts in order to read effectively. This adaptive technology has been around for 16 years or more, is affordable, and is easily implemented into computer systems. Here also there is no good reason for the Sequoia Edge II and ES&S iVotronic not to include this video access technology. The Diebold TSx also lacks many of the visual display enhancement adjustment features that should be available to make these voting systems more readable by low vision voters.

81. The Sequoia Edge II and ES&S iVotronic do not have voter-adjustable font size or magnification capabilities.

82. For the reasons discussed above, the Diebold TSx, Sequoia Edge II, and ES&S iVotronic DREs fall far short of meeting HAVA and Colorado's statutory standards. Enhanced display technologies for low vision users have been available for over 16 years and it should be easy to add this capability to computerized voting machines. As other DRE manufacturers have managed it, there appears to be no good reason that the manufacturers of the Diebold TSx, Sequoia Edge II, and ES&S iVotronic voting machines could not have easily adapted their designs to provide accessible visual display technology.

VVPAT Printouts Are Not Accessible to Many Persons with Disabilities

83. When attempting to read the output of the Voter Verifiable Paper Audit Trail ("VVPAT") printers in Diebold TSx, Sequoia Edge II, and ES&S iVotronic DREs, voters with low vision can only achieve useful magnification of the printout through external lenses. For nonvisual readers and for voters whose impairments prevent them from positioning themselves close enough to the VVPAT printer view window to read the printout, verifying their own vote on the verification paper printout is not possible. Using the audio read back feature of the DRE to confirm their electronic ballot marking in the DRE does not allow them to verify that their vote is recorded properly on the VVPAT paper printouts.

84. For example, the ES&S iVotronic voting system provides a VVPAT by means of a printer attached to each device that records on a rolling paper scroll the selections of voters as those selections are made. A voter verifies his or her vote on the audit trail by viewing the printout of that vote on the paper scroll through a small, "audit log window" on the printer. The ES&S iVotronic VVPAT, however, is not adaptable for, or useable by, many people with visual or motor disabilities. Blind voters cannot read the printout at all, and other visually impaired people might only be able to read this paper with the assistance of external lenses. Verification is also not possible for many voters with motor disabilities (*e.g.*, those who use wheelchairs) whose impairments prevent them from positioning themselves close enough to the VVPAT printer audit log window to read the printout.

85. Because these three DRE systems lack a VVPAT that all visually impaired or motor impaired voters can use, they do not afford the same opportunity for access and participation (including privacy and independence) as for other voters on these voting systems. Instead, the electronic voting machines give voters without visual or motor impairments a verification feature not made accessible to visually impaired or motor impaired voters.

86. With respect to the Diebold TSx, verification of the printout is also not possible when the tablet portion of the Diebold TSx is removed from the base, for example, to place it in a voter's lap or to take it outside for use in an automobile.

87. The VVPATs are really not accessible for most of the voters with disabilities or special needs. When representatives attempt to justify the lack of fully accessible VVPAT printouts by saying that it isn't important or doesn't matter because "other voting systems vendors don't have it," they are simply wrong. Adaptive technology to provide visually impaired and motor impaired voters with VVPAT capability is currently available, and systems such as the AutoMark Voter Assist Terminal (manufactured by ES&S) and VotePad (a tactile ballot sleeve technology), both of which I have tested, are able to provide accessible verification with standard paper ballots. The failure of the Diebold TSx, Sequoia Edge II, and ES&S iVotronic voting systems to include accessible VVPAT technology cannot be justified.

Experience Voting in Actual Elections on the Sequoia Edge II DREs

88. I have attempted to vote on Sequoia Edge II DRE machines in four separate elections. The first time, in March of 2004, the poll workers were never able to get any of the machines at our polling place rebooted with the audio-assist feature working. After 45 minutes of struggling with the systems, we gave up and I had to have someone else do my voting for me. Clearly these Sequoia Edge DREs were not designed correctly to be operated by poll workers lacking high levels of technical sophistication.

89. My experience voting on the Sequoia Edge II DRE with the audio-assist feature in the November 2004 election illustrates the problems that blind and visually impaired voters face when attempting to vote on Sequoia Edge II DREs.

90. After signing in, and getting my voter smart card, I had to wait eight minutes for officials to manage to reboot the audio voting machine. The polling officers had been using it for visual touch-screen voting, as there was a very long line and just five voting machines for our combined two-precinct polling place.

91. I had my notes in Braille. Because there was no table surface for the notes, the poll workers had to find me a chair so I could read my notes with the Braille on my lap.

92. The volume control on the front of the Sequoia Edge II keypad was not working well and resulted in scratchy and intermittent sound. By the time I got the volume set to where I could understand it, the introduction message had already finished the English instructions and was off into other languages. I was not sure what I should do, so I finally gave up and pressed the select button. This eventually got me to the language menu, where I was able to select English and get started with my ballot.

93. The first major problem I had was that the ballot on the Sequoia Edge II voting machine was not in the same order as the printed sample ballot. When my wife pointed this out to the chief poll worker, the poll worker was surprised to see the difference and said maybe that would explain why it was taking most voters longer than expected to vote. Because my notes were done in the order of the sample ballot, I had to do a lot of hopping around in my notes and be very thorough and careful listening to the machine. In contrast to what we had been told, the list of candidate names was spoken in alphabetical order.

94. It took me 30 minutes to work my way through the ballot and make my selections. After that, I had quite a bit of trouble getting into the review mode, to get a full list of all my selections. When I did, it went on and on, for 23 minutes, like a long uncontrolled drink from a fire hose. The review function read each item, and then, at the very end, said what my selection was for that item. It even threw in the details of what the fiscal impact would be, and took forever. This is completely backwards. It should announce the name of the item, then state my selection, and then read the rest of the information for that item. Also, I should have the control to press the arrow key to move forward or backward through the items, without having to listen to all the text about every item.

95. When I did find that I had made a mistake in my selections, I had to wait until the end of the whole review process to correct it, instead of being able to stop, make the change, and then continue with the review where I left off. I did not want to abort the ballot verification review to make a correction, and then have to start the long, tedious review all over again.

96. When I later attempted to change one of my selections from "no" to "yes," the machine would not let me just select "yes," until I had first gone to the unwanted choice and deselected it. This was very awkward and confusing. This is just poor human factors design for anybody, but especially for those using the audio assist feature. Many voters using the audio assist feature would not be able to navigate this difficult review and correction procedure.

97. At one point, as I was nearing the end of the ballot, I was dumped back into the language selection menu. I found out later that this was because the Sequoia Edge II has a timeout function that did this because I hadn't hit a key in quite a while. I hadn't hit a key for a while because it was taking a very long while to read out the long ballot summary! This is terrible human factors design. If a system is trying to present a helpful prompt when it senses an overly long delayed response from the user, it should never bounce the user off into a different place in the menu system. It might prompt the user, but it should then leave them at their previous position, to minimize confusion. Furthermore, the timeout should not begin until the system has finished reading out its message—in this case, after the whole ballot review summary. For a scary minute, I was afraid I had just lost my ballot and would have to start all over. I re-selected "English" and fortunately was returned to my previous location in the ballot.

98. An additional frustration was that the volume on some of the messages was so much lower than the rest of the messages that I had to turn up the volume, repeat the message, and then turn the volume back down before proceeding. The volume on all the messages should be normalized to make them the same.

99. From the time I signed in and got my voter smart card, it took eight minutes to reboot the machine as an audio voting machine, 30 minutes to make my choices, 23 minutes to review and verify, and another four minutes to make a correction and record my vote. Not counting the hour I had waited in line, it took me about 65 minutes to mark and record my ballot.

100. It would have taken even longer if I had been willing to wait, as prompted, until the end of each message to push the "select" button. The messages mislead some folks because they say something like, "at the end of this message, you can press the . . . ." This implies that you are supposed to wait until the speech message finishes.

101. I must emphasize that, in my opinion, my ability to navigate this process at all was due to my familiarity with computers and computer technology. I doubt that many blind or visually impaired voters would have been able to navigate it at all.

102. As an expert in the design of audio access technology, it is my opinion that the Sequoia Edge II system was incompetently designed.

103. The Sequoia Edge II audio review process is totally unacceptable and would cause most voters with disabilities to skip the review.

104. There were at least two times when I wanted to ask for help from the poll workers. One was during the confusion I encountered from the difference between the printed sample ballot and the DRE ballot. The other time was near the end of my ballot marking, when I had a lot of trouble getting the review started and then was trying to find and change a mistake I found during the review. Because the poll workers would not be able to look at a working visual display on my system, and didn't have any way to join me in listening to the audio output of the machine, I knew that I couldn't get much help from them (even though our head polling officer seemed very knowledgeable and helpful).

105. In November of 2005 I once again had a very frustrating experience attempting to vote with the Sequoia Edge II machine.

106. The polling officers (who were actually very pleasant) thought that they had booted the machine into audio mode first thing in the morning but they had not. Once they realized that it was not in audio mode, they could not figure out how to reboot the DRE into audio mode. After my wife read their manual and figured out the correct audio boot up process, she finally managed to get the machine properly rebooted and talking for them. This rebooting fiasco took 18 very frustrating minutes.

107. After the Sequoia Edge II voting machine finally started talking, it took me about six minutes to fill out the ballot, seven minutes to review my vote, and another minute to record my ballot and finish. Total time in front of the machine was 32 minutes. Luckily it was a short ballot with just eight choices.

108. After I initially made all my ballot choices, the Sequoia Edge II machine prompted me with a message that said something like "You are finished voting" instead of "If you are finished voting . . .," which is likely to cause some folks to walk away before their vote has been properly recorded. It should more obviously prompt with something like "If you are done making your choices, press select to record your vote." Many of the factory built-in prompts of the Sequoia Edge II audio-assist feature are similarly poorly worded and misleading or confusing.

109. Additionally, understanding the locally recorded November 2005 ballot messages was very difficult, because they had used a non-native reader who had a very thick foreign accent. Clearly, if I hadn't been very tenacious and hadn't taken my own computer expert along when I went to vote, I wouldn't have been able to vote privately.

110. More generally, I must emphasize that, in my opinion, my ability to independently navigate the Diebold TSx, Sequoia Edge II, and ES&S iVotronic voting processes at all was due to my familiarity with computers and computer technology. Many blind, low vision, and cognitively impaired voters would not be able to successfully navigate through the Diebold TSx's, Sequoia Edge II's, and ES&S iVotronic's hierarchical menu systems.

111. Additionally, as one familiar with the technology, I was far more likely than the typical voter using audio access to be able to figure out how Sequoia audio features worked and were structured, yet I had considerable difficulty that slowed the voting process. Many voters forced to use the audio-assist features might be embarrassed to tie up a voting machine for long periods, or not have sufficient patience, and therefore decide not to vote the entire ballot or not to fully review their selections before casting their ballot.

112. What I have heard from other voters, even sighted voters, is that they have often caught ballot marking mistakes in the review process. It is clear from this and from my own experience, that we really have to go through the review process in order to make sure that our ballots are accurate. The Diebold TSx, Sequoia Edge II, and ES&S iVotronic review processes are likely to cause most voters with disabilities to give up and skip the review.

113. The problems that poll workers have had properly setting up the Diebold TSx, Sequoia Edge II, and ES&S iVotronic voting systems for use by disabled voters show that the machines are not designed properly for operation by the general population of poll workers. The problem is due to flaws in the human factors design of the DREs, and should not be blamed on the poll workers' or voters' lack of technical expertise. Clearly, these Diebold TSx, Sequoia Edge II, and ES&S iVotronic DREs were not designed correctly to be operated in the real world by normal poll workers lacking high levels of technical sophistication and training.

114. The June 6, 2006, primary election in Santa Clara County was my fourth opportunity to attempt to vote on the Sequoia Edge II electronic voting systems. For 12 minutes, the poll workers struggled with trying to get the system talking. By watching the screen for them, my wife was able to tell them it wasn't setting up correctly. The poll workers tried repeatedly to program the voter ID card properly so it would cause my voting machine to talk. Fortunately, I remembered that, at the last Voter Access Advisory Committee meeting, a member of the ROV staff told me that the Sequoia ID card encoder did not show a menu choice for the audio voting mode. Our poll workers did not know that, just before the final step of encoding the ID card, they were supposed to issue a special menu command to bring up a hidden menu for selecting audio access mode.

115. After I explained this procedure for properly using the card encoder, they were eventually convinced to try it and were finally able to make me an ID card that actually worked and brought the machine up in the audio voting mode. What did happen, and what will happen in the general elections, to all the folks who were not told or did not remember enough to convincingly tell their poll workers how to encode their cards properly for audio access mode? They will not be able to vote using the Sequoia Edge II machines.

116. One of the plaintiffs in the California voter action, which is challenging certain DREs like this Colorado action, had to wait, after getting her voter ID card encoded, for the person in front of her to finish voting on the audio access Sequoia machine. When it was her turn to vote, the Sequoia Edge II rejected her voter ID card, as it had exceeded the 30-minute time-out limit. She had to have her card encoded several times more, before the poll workers could finally manage to get it properly set up to put the Sequoia Edge II machine in audio access mode.

117. After 12 minutes waiting for my Sequoia Edge II machine to be configured in audio mode, it took an additional 31 minutes for me to successfully navigate my way through the ballot marking procedure. It then took eight more minutes for it to play out the ballot review. At this point, I decided that I needed to change one of my votes to a write-in and that procedure took another seven minutes.

118. By the time the Sequoia Edge II system printed the paper trail and then spit out my voter ID card, I had spent a total of 59.5 minutes—nearly an hour—trying to vote privately.

119. There were several other problems I encountered while trying to vote on this Sequoia Edge II voting system. The voter ID card slot was hard to find, as it was located so low on the front bottom of the machine and lacked a good tactile guide bezel around its opening.

120. The locally recorded audio messages were distorted and poor quality from the speaker blowing on the microphone.

121. At least three times while I was voting the Sequoia Edge II timed out and put me back in the language selection menu, where it then required that I press the Select key twice to exit the language menu and return to my previous position in the ballot.

122. Since the June 2006 primary election, I've heard from other voters who voted in precincts of Santa Clara County that the precincts were using the cardboard privacy panels from the old punch-card booths, in hopes that would afford a better privacy shield than the flimsy panels that normally are attached to the sides of the Sequoia Edge II units.

123. Because of the width of the combined printer and Sequoia Edge II touch screen unit, the printer would have to be disconnected and removed from the touch-screen device and placed in a wheelchair voter's lap to enable that voter to vote. A motor-impaired friend of mine who tried this found that he had to have a poll worker stand behind the Sequoia Edge II touch-screen unit and hold up its back end to keep it from falling off his lap while he voted. The Sequoia Edge II is clearly not designed to work in the lap of someone in a wheelchair.

124. The legs of the Sequoia Edge II stand appear to be only about 16 inches apart, too narrow for some wheelchairs.

125. When the system printed my vote on the VVPAT roll-to-roll printer, I asked my wife to take a look at it, to verify my vote for me. It turns out that if I am using the audio access feature and have a multi-page ballot, the printer prints out the whole ballot in one shot, and then clears it out of the viewing window, without any break to stop and permit me to have a sighted friend read the paper trail for me. When sighted folks are printing their ballot on the VVPAT without audio, it only prints a single printer page's worth at one time and then pauses for the user to press a button to make it print the next page, after the voter is ready.

126. Because the manufacturer of the Sequoia Edge II system knows that blind voters will not be able to read and verify the paper trail themselves, the manufacturer incorrectly assumes that all audio voters want the whole ballot printed out without any pauses for viewing by anyone.

127. One of the Sequoia Edge II voting machines in our polling place was broken and taken out of service. Luckily for me, it was not the audio access voting machine.

128. In summary, the setup of the Sequoia Edge II in audio access mode is still too complicated for the average poll worker; marking and reviewing the ballot takes a very long time for the audio voter; the physical privacy shielding is even worse than it used to be with punch-card systems; and audio voters do not have any way of verifying the paper audit trail privately or otherwise.

129. I am aware that Diebold, Sequoia, and ES&S all represent that they are working on making future improvements to the audio prompts and other capabilities of their DRE machines. However, like the two-switch input-control feature and other access options that have been promised by these vendors, these possible future features are still not available on our real voting systems in our real polling places today.

130. As my own experiences prove, it is certainly possible for some tenacious disabled persons to get through the voting process successfully on these Diebold TSx, Sequoia Edge II, and ES&S iVotronic systems. However, that experienced computer and access technology users like myself have had such frustrating experiences trying to use the Diebold TSx, Sequoia Edge II, and ES&S iVotronic DREs, clearly indicates that these systems have not been designed to provide appropriate access for the general disabled population.

131. In summary, it is my opinion that the Diebold TSx, Sequoia Edge II, and ES&S iVotronic DREs are not voting systems that meet HAVA and Colorado statutes' disability accommodation requirements. The Diebold TSx, Sequoia Edge II, and ES&S iVotronic systems would require significant redesign to comply with federal and state legal requirements.

I declare under penalty of perjury under the laws of the State of Colorado that the foregoing is true and correct and that this declaration was executed on June 27, 2006, at Albuquerque, New Mexico.

Noel H. Runyan