ELECTION REFORM: AUDITING THE VOTE

HEARING

BEFORE THE

SUBCOMMITTEE ON ELECTIONS

COMMITTEE ON HOUSE ADMINISTRATION

HOUSE OF REPRESENTATIVES

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

MEETING HELD IN WASHINGTON, DC, MARCH 20, 2007

Printed for the use of the Committee on House Administration

Available on the Internet:
http://www.gpoaccess.gov/congress/house/administration/index.html

ELECTION REFORM: AUDITING THE VOTE

HEARING

BEFORE THE

SUBCOMMITTEE ON ELECTIONS

COMMITTEE ON HOUSE ADMINISTRATION

HOUSE OF REPRESENTATIVES

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

MEETING HELD IN WASHINGTON, DC, MARCH 20, 2007

Printed for the use of the Committee on House Administration

Available on the Internet:
http://www.gpoaccess.gov/congress/house/administration/index.html

U.S. GOVERNMENT PRINTING OFFICE

35–804 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

JUANITA MILLENDER-MCDONALD, California, *Chairwoman*

ROBERT A. BRADY, Pennsylvania
ZOE LOFGREN, California
MICHAEL E. CAPUANO, Massachusetts
CHARLES A. GONZALEZ, Texas
SUSAN A. DAVIS, California
VERNON J. EHLERS, Michigan
Ranking Minority Member
DANIEL E. LUNGREN, California
KEVIN MCCARTHY, California

SUBCOMMITTEE ON ELECTIONS

ZOE LOFGREN, California, *Chairwoman*

JUANITA MILLENDER-MCDONALD, California
CHARLES A. GONZALEZ, Texas
SUSAN A. DAVIS, California
KEVIN MCCARTHY, California
VERNON J. EHLERS, Michigan

AUDITING THE VOTE

TUESDAY, MARCH 20, 2007

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

The subcommittee met, pursuant to call, at 2:50 p.m., in room 1309, Longworth House Office Building, Hon. Zoe Lofgren (chairwoman of the subcommittee) presiding.

Present: Representatives Lofgren, Gonzales, Davis of California, McCarthy, and Ehlers.

Also Present: Representative Holt.

Staff Present: Tom Hicks, Election Counsel; Janelle Hu, Professional Staff Member; Matt Pinkus, Professional Staff/Parliamentarian; Kristin McCowan, Chief Legislative Clerk; Gineen Beach, Minority Counsel; and Peter Sloan, Minority Professional Staff.

Ms. LOFGREN. Welcome to everyone. First, apologies for our tardiness, for some reason as soon as there is a Election Subcommittee notice, the House calls at least 5 votes and makes us late. And so obviously, we have to go over and do our duty of voting. But it does put us in a delay mode and we do apologize.

Last week, we had a hearing on election reform and learned about some of the issues surrounding the tools of voting machines and software as well as access to those machines for all voters.

This week, we shift focus to what happens when the polls close, auditing. The Help America Vote Act, or HAVA, addressed machines and established new procedures for voting lists and registration, but auditing was not addressed. Post election audits are a tool to increase voter confidence in the election process. But there is no national standard for auditing in Federal elections. There are States, such as California, where the paper count takes precedence over the electronic one, or other States like Nevada are the reverse.

Discrepancies are not just about paper or electronic counts. It also goes to the extent of audits. Connecticut has performed post election audits using 20 percent of precincts. Other States are as low as 1 percent of precincts. In addition to the extent of audits, they need to be conducted so they are publicly observable. And audits must, as we know, also be entirely random to avoid the possibility of tampering.

Greater transparency through increased election scrutiny is not a bad thing, and having a voter verified paper trail with an automatic routine audit may go a long way to increase voter confidence and to deter fraud.

It is no secret that a number of recent elections have been determined by a very small difference of votes. And a handful of these are still in dispute. A failure to have paper records that can be audited could ultimately call into question the validity of a very close election. And it may be that an established national process for the audit of Federal elections would be worthwhile.

I would like to call on the ranking member, Mr. McCarthy, for his opening remarks, and also invite the other Members to submit statements for the record. Mr. McCarthy.

[The statement of Ms. Lofgren follows:]

House Administration
Elections Subcommittee

Election Reform: Auditing Federal Elections
Tuesday, March 20, 2007

Opening Statement

Last week we had a hearing on election reform and learned about some of the issues surrounding the tools of voting, machines and software, as well as access to those machines for all voters. This week, we shift focus to what happens when the polls close: auditing.

The Help America Vote Act (HAVA) addressed machines and established new procedures for voting lists and registration, but auditing was not addressed. Post-election audits are an essential tool to increase voter confidence in the election process. Unfortunately, there is no national standard for auditing in federal elections. There are states, such as California, where the paper count takes precedence over the electronic one while other states like Nevada are the reverse.

Discrepancies are not just about paper or electronic counts; it also goes to the extent of audits. Connecticut has performed post-election audits using 20% of precincts but other states are as low as 1% of precincts.

In addition to the extent of the audits, they need to be conducted so they are public observable. Audits must also be entirely random to avoid the possibility of tampering.

Greater transparency through increased election scrutiny is not a bad thing. Having a voter-verified paper trail with an automatic routine audit will go a long way to increase voter confidence and deter fraud.

It's no secret that a number of recent elections have been determined by a very small difference in votes and a handful of these are still in dispute. A failure to have paper records that can be audited could ultimately call into question the validity of an election. An established national process for the audit of federal elections is needed.

Mr. MCCARTHY. Well, I appreciate the Chairwoman for calling this hearing on election audits. I do believe that all Members of this panel as well as our colleagues in the House are dedicated to ensuring that Federal elections are conducted and tabulated in a free and fair manner. I do want to make sure, though, that the Federal interest in this issue should not cloud the work of the State and local jurisdictions and I am happy that we have two States here, Ohio and Arizona, that tabulate and do an audit as well, so we will hear from them on the ability that we can work together and make sure we have fair and honest elections. Thank you.

[The statement of Mr. McCarthy follows:]

Committee on House Administration
Subcommittee on Elections
Federal Audits
March 20, 2007

Ranking Member McCarthy's Opening Statement

I appreciate the Chairwoman for calling this hearing on election audits. I believe that all members on this panel, as well as our colleagues in the House, are dedicated to ensuring that Federal elections are conducted and tabulated in a free and fair manner.

But Federal interest in this issue should not cloud the work of state and local jurisdictions on ensuring that voters have a reasonable certainty that the votes they cast were counted correctly. I am pleased we will be taking testimony from witnesses in Ohio and Arizona that can provide first-hand accounts to the auditing procedures in their jurisdiction, and to gauge their reaction and experiences with their own state auditing process. But we are getting input from two states that have experience with manual audits after an election. Are the approaches that the various states have been using beneficial in ensuring vote count results reliability, especially when comparing the electronic tally with the hand recounts? When there is a discrepancy, which count should be given more weight, an electronic count done by pre-certified software that might nonetheless have a bug in it, or a hand count of ballots that are being done by weary volunteers and election officials? Who are the best people to audit? What is the comfort zone that election officials have with the amount of ballots subject to an audit, with the resources they have to report the results of an election in a timely manner, after the election and under state law as to when an election is certified? Without seeing what the background is in the local, state, and federal arenas right now, it is difficult to paint a picture of the extent of federal legislation, if any, would be necessary, especially if done at the expense of federal taxpayers. Thus, I would urge additional subcommittee scrutiny on this as well as the other subject areas on elections that the Chairwoman has correctly recognized needs a public hearing.

Currently, we have 27 states that require paper trails, with 13 more considering that approach, in addition to the 15 states that have some sort of requirement of manual audits of paper ballots or trails. As at least three of my colleagues on this subcommittee are familiar, my home state of California has required a public audit of one percent of randomly chosen precincts after every election. These audits are conducted by local election officials and the audit occurs by hand. This approach is different than the approaches of other states, but all have the same goal in mind, to administer free and fair elections. I believe we must approach these hearing with that perspective in mind and be mindful of our states' efforts when conducting these oversight hearings.

I thank the witnesses for joining us today to examine these critical issues and I look forward to hearing their testimony and answers to our questions.

Ms. LOFGREN. Thank you. I would just like to note for the record that there was some confusion on witness notification and submission of testimony, and we are going to strive at the next hearing to have all our testimony submitted within the 48 hours that is specified in the rules and make sure that everything is shared as promptly as possible between the sides.

I would like now to call upon our first panel, and, we have Mr. Ion, is that how it is pronounced? Sancho, who is the supervisor of elections from Leon County Florida. He was elected to his first term as supervisor of the elections in November of 1988, re-elected in 92, 96, 2000, 2004 and serving his fifth term in—as of January second 2005. He has a JD from Florida State University Law School, a bachelor's degree from Stetson University.

And we also have Mr. Matt Damschroder, who is the director of the Franklin County Board of Elections. And Mr. Damschroder has been the Director of the Franklin County Board of Elections since 2003 and serves as the president of the Ohio Association of Election Officials. And he was the executive director of the Franklin County Republican Party until his appointment to the Board of Elections.

STATEMENTS OF ION SANCHO, SUPERVISOR OF ELECTIONS, LEON COUNTY, FLORIDA; AND MATT DAMSCHRODER, FRANKLIN COUNTY BOARD OF ELECTIONS

Ms. LOFGREN. We welcome both of you and we have a light system here. We will ask that you summarize your written statements which we will have and submit for the record and try and give your oral remarks in about 5 minutes that will allow for questions. So if we may ask, Mr. Sancho first and then the other witness.

STATEMENT OF ION SANCHO

Mr. SANCHO. Thank you, Chairwoman Lofgren, Ranking Member McCarthy and committee members. Thank you for the opportunity to testify today. My name is Ion Sancho. I am the elected supervisor for elections for Leon County, Florida. I am a member of the International Association of Clerks, recorders, election officials and treasurers, and the election officers, the two largest professional associations for election officials in the country. I have no party affiliation.

In my testimony today, I will focus the problems Florida has encountered over the past 6 years and how our audits—or more accurately, the lack of audit—have contributed to the current crisis in confidence Floridians have in their electoral system today, a crisis of confidence that is so critical that the incoming governor, upon taking office, stated that in the State of Florida, there will be—there will be a paper trail for every vote.

And that is a sea change from the previous administration.

What are audits? One dictionary definition refers to an audit as an official examination and verification of a accounts and records. Another calls it a methodical examination and review. I would like to say that the reason that I had to resort to the dictionary is that audits have no definition under Florida law. Because Florida does not conduct audits. Before the election, we have to do a series of tests, which we call logic and accuracy, and after the election, we

do a logic and accuracy that ensures that the machine can count a test step. But we never audit actual ballots or votes. And so as an election official, I had to resort to the dictionary to describe an audit.

Which leads me to directly to the 2000 elections. In Florida, audits for any election, again, as I have mentioned, are not required.

The closest thing that we have had in Florida election law to an audit was our pre-2000 recount provisions in chapter 102, which, depending on the closeness of the contest, could mean that every ballot had to be manually examined.

These recounts are generally rare events. In my almost 20-year career, I have overseen four of them, and only one of these, the presidential race of 2000, involved a Federal race, and that recount, the only audit that we could use was terminated by the United States Supreme Court. All of us in Florida were embarrassed by what happened, including election officials. And this embarrassment, which the Miami Herald recorded at 70 percent dissatisfaction with our electorate, forced our public policy makers to act.

The governor ordered a bipartisan task force, which held hearings across the State and produced 35 excellent recommendations, including audits. But audits, recounts, voter intent, were all discarded out of that task force series of recommendations and substituted in those for those audits and recounts was the assumption that since voting machines could never make a mistake, it was illogical then to audit any result that was produced by voting machines. And this is the current State of Florida law today.

Let me tell you that if we were going to have the same kind of statistical dead heat in Florida in 2008, we would have less than 1 percent of the ballots examined under current law. Why? Because under Florida law, the only ballots which can be examined in an audit are those ballots which could not be read by voting machine.

That means every machine readable ballot is out of bounds in a recount to examine.

In the last election, only 500 ballots out of over 92,000 ballots cast would be examined under a Florida recount, roughly less than 1 percent of the ballots. Again because only these number of ballots, the overvotes and undervotes and optical scan ballots, either by those jurisdictions who use paper ballots in the precincts or those ballots received by the election official through the mail which are on paper, only those ballots which are nonmachine readable could be manually audited.

Ms. LOFGREN. Mr. Sancho, the red light means your time is up, so could we ask you to wind up and we will go to our next witness?

Mr. SANCHO. All right. I would urge this body to require that mandatory random and manual post election audits be made the law. Without them, no citizen, State or Federal in terms of the races that they focus on, can actually have any validity under Florida's current statutory scheme that is, in fact, their votes are being counted. Thank you.

Ms. LOFGREN. Thank you very much for that testimony. And as I mentioned earlier, your complete statement will be made a part of the record as well as the questions that follow.

Mr. DAMSCHRODER, now it is your turn, and I probably should have said when the yellow light goes on that means you have a little time left to summarize.

STATEMENT OF MATT DAMSCHRODER

Mr. DAMSCHRODER. Good afternoon, Madam Chairwoman and members of the committee. Franklin County is the most populous county of Ohio's 15th congressional district. And during the 2006 congressional election cycle, the 15th congressional district election resulted in an official margin of victory of less than one half of one percent or less than 1,055 votes. That general election was administered in Franklin County using direct recording electronic voting machines, or DREs, with a voter verified paper audit trail.

In 2004, the Ohio General Assembly had enacted legislation requiring the VVPAT to be included in all DRE's beginning in 2006. I was the only election official in Ohio who testified in support of VVPAT technology. But I had two concerns with Ohio's legislation. And they are the two concerns that I have with H.R. 811.

First, the VVPAT should not be, in my opinion, the ballot of record. With the VVPAT as the official ballot, it is possible that an otherwise properly cast and accurately recorded ballot on the DRE might not be recounted in a close election due to paper jams or poll worker error loading the paper backwards. The question what constitutes a vote, having long been determined in Ohio for punch cards and optically scanned paper ballots, has seemed wrong to me at the time and wrong to me now that we would institute a new voter intent question that could cause a voter's properly cast and accurately recorded vote to go uncounted.

Second, the VVPAT requirement should go into effect only after the Election Assistance Commission had developed standards for the function and operation of the technology.

I am concerned that by enacting portions of this legislation, Congress might be making precisely the same mistake that Ohio made by mandating changes to the technology by date certain before operational standards are established and the technology is fully developed and tested.

Essentially in Ohio and in Franklin County specifically, our $14 million investment partially included HAVA funds and partially including local taxpayer funds would likely have to be dumped because our VVPAT technology does not conform to the requirements of this legislation.

Beginning with our first use of the VVPAT in a special election of February of 2006, we began voluntarily conducting audits of the VVPAT to the electronic record.

As a part of that, we determined that there were instances where the paper printers did jam or that poll workers did make errors in loading the paper tapes backwards. So as we prepared for the recounts, the mandatory recount in the 15th congressional district election, we knew that there were going to be problems and with no definition in Ohio law from the Secretary of State in answering that very important voter intent question on the VVPAT, the Board of Elections engaged both of the campaigns to basically create ground rules for the conduct of the recount of how we would treat a ballot in the event that we came to a jam or a blank tape.

The hand tally of the VVPAT for this Federal recount took 2,000 employee hours. And again, that was to hand tally 10 percent of the total votes in Franklin County.

I would like to bring one specific instance to the committee's attention that demonstrates the importance of clear and objective guidelines to define voter intent on the VVPAT. On one particular paper tape, the recount team encountered a paper jam and there was no indication on the paper tape that the voter's voting session had ended in a ballot properly being cast. At the conclusion of the recount of that tape, the total number of hand tallied votes excluding the so-called jammed vote on the paper tape equaled the total number of votes cast on the machine. To further verify that the so-called jammed vote should not be counted, the recount team examined the ballot image log and the electronic event log, both of which validated that there were only the specified number of ballots cast in the machine. And the event log actually showed that at the time displayed on the paper tape that the printer had jammed.

Additionally, the poll workers followed their responsibilities and noted in their records that a paper tape had jammed, that they cancelled the ballot and allowed the voter to vote on a different machine.

When using VVPAT technology which introduces new question of voter intent as I described, vague and subjective language, such as 811's phrase, preponderance of evidence or clear and convincing evidence is an open invitation to litigation. In Franklin County, that could have meant that litigation would have required weeks beyond the end of the recount and that possibly a representative from the 15th congressional district not being seated when Congress convened, also look towards 2008, it could possibly mean that our recounts and other audits would not be concluded by the time the Federal electors are seated.

Our experience in this recount demonstrates the accuracy of electronic voting systems and the benefit of State and local control over election audit recount definitions and procedures.

[The statement of Mr. Damschroder follows:]

UNITED STATES CONGRESS
HOUSE OF REPRESENTATIVES
Committee on House Administration
Elections Subcommittee

Tuesday, March 20, 2007

Good afternoon Madame Chairman and Members of the Committee. I am Matthew Damschroder, Director of the Franklin County Board of Elections in Columbus, Ohio and President of the Ohio Association of Elections Officials.

Franklin is the majority county of Ohio's 15th Congressional District. During the 2006 Congressional election cycle, incumbent Republican Deborah Pryce faced Democrat County Commissioner Mary Jo Kilroy in a contest that resulted in an official margin of victory for Congresswoman Pryce of less than ½ of 1% or 1,055 votes out of more than 222,000 ballots cast thus requiring an automatic recount.

The Franklin County election was administered using the ES&S iVotronic direct recording electronic voting machine, or DRE, with a voter verifiable paper audit trail, or VVPAT. There were 45,684 ballots cast on optically scanned paper absentee ballots and 150,186 ballots cast on 2,341 VVPAT DREs. To my knowledge, it was the closest Congressional election in the Country that used VVPAT DREs.

The use of DRE technology is not new for Franklin County: from 1992 to 2005 elections in Franklin County have been run on paperless DREs. Prior to 2006, both candidates had been elected and re-elected on this technology multiple times.

In 2004, the Ohio General Assembly enacted legislation requiring VVPAT technology to be included with all DREs beginning with the first federal election of 2006. I provided testimony in favor of VVPAT technology. But I offered two strong cautions that were left unaddressed in Ohio's legislation. I have the same concerns with HR 811.

First: the VVPAT should not be the ballot of record; it should be used only as an audit device to prove the electronic record. With the VVPAT as the official ballot it is possible – and this was shown to be true during the 15th Congressional District recount – that a ballot having been otherwise properly cast and accurately recorded by the DRE might not be re-counted in a close election – such as the 15th Congressional District – due to paper jams or poll worker error loading the paper backwards. The question "what constitutes a vote" having long been determined in Ohio for punch cards and optically scanned paper ballots, it seemed wrong to me that we would introduce a new voter intent question that could cause a voter's properly cast and accurately recorded vote to go uncounted.

Second, the VVPAT requirement should go into affect only after the Election Assistance Commission (EAC) has developed standards for the function and operation of the technology. At the time Ohio passed its VVPAT legislation, the EAC had only just recently convened the first meeting of the Technical Guidelines Development Committee

(TDGC). It seemed backwards to me that Ohio would spend millions of taxpayer dollars to implement a technology that had not yet been developed nor tested and had no federal standards regulating its operation and function. I am concerned that by enacting portions of HR 811, Congress will be making precisely the same mistake that Ohio made by mandating changes to technology by a date certain before operational standards are established and the technology is fully developed and properly tested prior to deployment.

In absence of clear guidance in law or from the Secretary of State on the manner and standards by which a VVPAT recount should be conducted in Ohio in preparation for the mandatory recount of the 15th Congressional District, I met with attorneys for each of the campaigns to define the terms of the recount.

We agreed that, due to the narrow margin of victory in the Congressional contest, it was necessary to exceed the minimum percentage of votes to be hand-recounted. The Secretary of State's administrative guidelines require 3%. Our agreement required 10%.

Additionally, we agreed that if the VVPAT was illegible or blank that the Board, in the presence of observers from each of the campaigns, would rely upon the electronic Ballot Image Log and Event Log to determine the indecipherable ballot or ballots at the point of the jam or blank tape.

Precincts containing 10% of the total votes were randomly selected by a representative of each campaign prior to the start of the recount. 49 precincts were selected containing 14,723 total ballots cast on 271 machines.

The hand tally of the VVPAT took five teams of four Board employees, each with two Republicans and two Democrats, five days to accomplish the hand tally phase of the recount.

I would like to bring one specific instance to the Committee's attention that demonstrates the veracity of the electronic voting devices and the success of policies and procedures agreed to by the two campaigns, which protected the integrity of the process.

On one particular paper tape, a recount team encountered a printer jam. The voter had clearly begun a voting session and had cast a vote for candidates for various offices when a printer jam appeared to have occurred after the voter had cast a vote for a candidate in the 15th Congressional District contest. There was no indication on the VVPAT that this voter's voting session had ended in the ballot being properly cast.

Recount staff did not count that vote at that time, waiting instead to see if the total ballots counted, less the jammed ballot, equaled the public count, or total votes, on the machine thus indicating that the ballot was indeed not electronically cast. At the conclusion of the recount of that tape, the number of total hand-tallied votes, excluding the so-called jammed vote on the VVPAT, equaled the total number of votes cast on the machine.

To further verify whether or not the "jammed vote" should be counted, the recount team hand-counted the votes electronically recorded in the machine's ballot image log. The ballot image log matched exactly with the VVPAT.

Additionally, the machine's electronic Event Log was examined. The Event Log showed that the voting session in question had begun at the exact time printed on the paper tape and further showed that a printer error had occurred and that the password-protected service menu had been accessed by a poll worker and the ballot in question cancelled.

Finally, the recount team examined the poll workers' Election Day records for the precinct. As instructed, the poll workers had notated that at the time printed on the VVPAT and recorded in the Event Log, a printer error had occurred on the machine in question and that the poll worker had rightly cancelled the voter's ballot and moved the voter to a different voting machine to begin a new voting session. They also noted that at a later time, a machine technician had arrived and fixed the jam so that voting could continue on the previously jammed voting machine.

At the conclusion of the recount, not one vote that had been electronically recorded as a normal ballot changed as a result of the hand tally of the VVPAT. The only votes that truly changed – a total of 8 – were on the optically scanned paper absentee ballots. In every instance, the VVPAT record precisely matched the electronic record of the DRE. Not one vote that had been recorded electronically changed as a result of the inspection of the VVPAT.

The recount of the Franklin County portion of the 15th Congressional District – just one of the three Congressional Districts that overlap into our county – consumed nearly 2,000 person hours over the course of seven days.

One important outcome of this recount – beyond officially re-counted and certified election results – was the knowledge of the impact of Ohio's recount provisions using VVPAT DREs in a close federal election.

When using VVPAT technology, which introduces new questions of voter intent as I have already described, vague and subjective language, such as 811's phrase "preponderance of the evidence" is an open invitation to litigation. "Preponderance of the evidence" to one observer or election official of a properly cast electronic vote that does not legibly appear on the VVPAT due to a printer jam or backwards-loaded paper tape will not likely be a preponderance of the evidence" to another in a politically-charged, narrow-margin recount.

I believe that the question of voter intent on a VVPAT is better left to the individual States to decide in precisely the same manner that the Federal Government has left to them the same question for optically scanned and punch card paper ballots.

Franklin County's recount was only concluded as efficiently as it was because of the local agreement reached by the Board and the two campaigns that defined voter intent

questions on the VVPAT before the recount commenced. Had these questions gone unanswered, litigation would have almost certainly resulted, and it is possible that Congress would have been unable to seat a representative from the 15th Congressional District at the time it convened this past January. Federally codifying subjective language on such an important issue as voter intent is an invitation for further eroding of voter confidence in our Country's exceptional system of elections administration in 2008.

Franklin County's experience in 15th Ohio Congressional District recount, as well as the three other recounts conducted of the 2006 General Election and the three subsequent voluntary audits of the paper tapes to the electronic record conducted by the Board and the local newspaper, demonstrates the accuracy of electronic voting systems and the benefit of State and local control over election, audit, and recount definitions and procedures.

Ms. LOFGREN. Thank you very much and congratulations on having a precisely 5-minute statement. I would like to begin the questions, if I may, and I will start with Mr. Sancho.

You have been an election official for a long time and have had substantial experience. In your experience, do you have an opinion on what voting system or machine makes conducting an audit easier, more transparent and accurate?

Mr. SANCHO. Yes, I do. I believe that a document—right now the only thing we have is paper, marked by the voter's own mark, in their own handwriting, is the kind of evidence that would allow me to do a complete audit.

I got into the area of elections in 1988 because in 1986 I ran for a local government position, and our supervisor of elections negligently programmed the voting machines so that they jammed on Election Day—through, it was not nefarious it was just negligence. But it meant that upwards of 5,000 Leon County voters could not vote on that Election Day. And when I ran for and got that position 2 years later, the number one thing on my agenda was to create a voting system and a process that would allow the voters to know what the votes were, even if I negligently programmed the voting machines.

So I wanted a system that would have a backup to the technology that I could confirm the validity of the votes. And that led me to optical scan voting technology, which is emerging in the late 1980s and early 1990s. And it was a technology that would allow every voter to mark that paper ballot and then I could scan them and get the result to the media quickly and to the candidates. But if there were any disputes over my handling of the ballots or of the election workers handling of the technology, the evidence resided in the form of optical scanned ballots which no one need use technology to get a 100 percent accurate count. And that is what we selected on in 1992. And the results are clear. In the 2000 botched election, Leon County had a residual or error rate of less than 1 fifth of 1 percent.

My neighboring county had an error rate of 12.4 percent, which means that only 86 percent of the citizens that tried to vote in the presidential race actually even ended up having their vote properly recorded. That—all of us that used the optical scan technology in Florida had an error rate of less than 1 percent.

And we were able to recount our ballots without a problem. The punch card and the central count systems failed the citizens and they were banned.

Ms. LOFGREN. The governor of your State has recently made—is he—is the State of Florida moving toward that system?

Mr. SANCHO. We are making steps in a very, very good direction. House Bill 2166, which was introduced by Senator Villalobos, at the behest of the governor would replace every touch screen voting machine at the precinct on Election Day with an optical scanner. And that is a very excellent first move.

Ms. LOFGREN. Let me ask you, you have—correct me if this is wrong—but my understanding is that you did some testing to see whether voting machines could be hacked or not hacked. Could you describe or report to us on your findings in that regard?

Mr. SANCHO. Yes. After the 2004 election, I was approached by a British journalist who had been observing elections across the country, and I guess I struck him as sort of an honest type of guy. And he said, I think we can hack your voting system. And I said I don't think so. But he said, would you be open to having an independent test to see whether or not your system would be compromised? And I thought about it for a while. We had some negotiations. And I answered yes.

And what we found over the course of six tests that took 11 months to conduct, was in fact a huge, huge security flaw in the process that would allow anyone with insider access to actually prestuff the electronic ballot box and have those numbers alter the outcome of an election. And it would not be detected in the normal canvass process.

This was shocking to me. And quite frankly, it confirms my own sense that even when you are using a paper-based system, unless you actually audit it, it can be vulnerable to a whole host of security attacks which the systems administrator would not even be aware is occurring.

Ms. LOFGREN. I am going to turn it over to my ranking member, Mr. McCarthy.

Mr. MCCARTHY. Thank you, Madam Chair.

Question for Franklin. Ohio has automatically, if you are in the half percent to 1 percent, you do the audit.

Mr. DAMSCHRODER. That's correct.

Mr. MCCARTHY. Now you have raised some good points here because you have gone through a little legislation that we may bring up later with the VVPAT. You said in your statement that the paper should not be the ballot of record.

Mr. DAMSCHRODER. That is correct.

Mr. MCCARTHY. Could you elaborate on that a little more and why?

Mr. DAMSCHRODER. My belief is that the voter verified paper audit trail should not be the ballot of record, and the reason I believe that is when you compare an electronic touch screen system to an optical scan system, with the optical scan as Mr. Sancho mentioned, the voter as marking the ballots themselves, the electronic system in Franklin, Ohio with the voter verified paper audit trail the voter is marking the ballot electronically, and they are verifying that paper record.

In situations with a recount of the—in Ohio of an optical scan system, you hand tally a small universe. The minimum requirement is 3 percent of the optical scan paper ballots. And then you run them through the tabulator and compare the hand tally to the electronic tabulator result. If they match, then you rerun all of the ballots electronically. Basically, the hand audit of the paper is to prove the veracity of the electronic.

To me, I believe that it is not recommended to create a higher standard for an alternate voting system so that we should use the voter verified paper audit trail as it has been named in Ohio, and as it is named, I believe, in this legislation for that precise purpose to audit the electronic results. When the paper ballot becomes——

Mr. MCCARTHY. So you are saying the paper should not be the final decision maker?

Mr. DAMSCHRODER. Should not be, because as I shared in my testimony, in some instances, the paper jams——

Mr. MCCARTHY. You said that paper jammed and it shows that it jams and the people did what was right even though you trained them, you gave them enough training and computer showed that it did jam?

Mr. DAMSCHRODER. Correct.

Mr. MCCARTHY. So did that ballot get counted properly and it wasn't double-counted?

Mr. DAMSCHRODER. It was not double-counted because when the paper jammed, the machines are designed, such as the machine will not allow the voter to continue casting ballot when the paper is jammed or is not present. So when the, in this instance, when the printer jammed, the voter noticed that the machine stopped allowing him to vote or her to vote, notified a poll worker. The poll worker cancelled the ballot on that machine and took the voter to a different machine where she could cast her ballot and the jammed machine was not used again until a technician could come and unjam the paper.

Mr. MCCARTHY. Now you said it took 2,000 hours to do this audit or recount.

Mr. DAMSCHRODER. Correct.

Mr. MCCARTHY. And you believe audits are good.

Mr. DAMSCHRODER. Yes, I do. And that is why we did three audits before the 2006 general voluntarily.

Mr. MCCARTHY. How many races in Ohio come within 3 percent?

Mr. DAMSCHRODER. I don't know for sure. In Franklin County, it is very few. This congressional district was very unique in the political balance of the jurisdiction, also the characteristics of the contest.

Mr. MCCARTHY. Would you audit every race?

Mr. DAMSCHRODER. I would not. In the situation of the previous audits that we did, we randomly selected a handful in two of the contests that were a single issue. In the primary, we randomly selected, I think, about a dozen contests of the probably 50 that were on the countywide ballot and tallied those from 3 percent of the machines, so I don't believe it is necessary to tally the entire universe. I am not a statistician, but all the statisticians that I have spoken with lead me to believe that with that form of mathematics, you can test a small universe to learn with virtual certainty the characteristics of the entire universe.

Mr. MCCARTHY. Fortunately, we have a person that knows math very well on the committee that could probably answer that for us. But let me ask one question to the individual from Florida. Would you audit every race?

Mr. SANCHO. No, I would randomly select races, but I think that you with particularly the focus here at Federal races, I think you have to look at the Federal races that has to be included one of the Federal races.

Mr. MCCARTHY. Would you pick it based upon the difference in the race? Or would you pick every Federal race? Would you say if a race came between 3 percentage points, 5 percentage points, 1 percentage point, 10 percentage points?

Mr. SANCHO. Well, in Florida, we basically have no more than three Federal races on any particular general election ballot. So if you wanted to do all the feds, you could do that. The 2,000-hour time frame that was described by Matt is essentially a series of 4, I believe it is 5, 4-person teams Matt?

Mr. DAMSCHRODER. Mmh-hmm.

Mr. SANCHO. And how long did that take you to do?

Mr. DAMSCHRODER. Seven days.

Mr. SANCHO. Seven days, 5 four-person teams, the number 2,000 sounds large, but an audit that takes 7 days that examines 10 percent of the vote in the largest jurisdiction in Ohio, actually I commend him on doing it within 7 days.

Mr. MCCARTHY. So could you, timewise, if you were required to do every Federal race, could you do it?

Mr. SANCHO. Absolutely in three races, random selection—and not—I would like to say I think you have to do a—my own analysis of the statistics involved, if the race is very close, you would not want to use the same number to statistically sample a race in which the margin is 25 percent apart. I think a tiered system, the closer the race is, the larger your sample is going to have to be if you are going to get the level of confidence—and in my mind, you are talking about 99 percent plus confidence rate—in order to establish that what you do has meaning.

Because that is really what we are trying to accomplish here. We are not trying to just do an audit so that we do an audit and we have done an audit. We are trying to do an audit so that the individuals involved in the race, their supporters and everyone concerned can know with confidence that result is the result.

Ms. LOFGREN. I would like to call Judge Gonzalez, our colleague from Texas.

Mr. GONZALEZ. Thank you, very much, Madam Chairwoman. And the question will go to—is it Damschroder?

Mr. DAMSCHRODER. Damschroder. Correct.

Mr. GONZALEZ. I am new to the committee and appreciate this opportunity. It is a education for all of us, the general public out there many times will be confusing audit with recount and the manner in which you would conduct that. I guess my question really goes—and I will be asking Mr. Sancho a question in a minute—but regardless, it appears that you are still depending on a paper trail to serve a very important function even in the auditing process, because by your testimony a minute ago, it would be the paper ballot or the printout from the electronic recording of the vote that would basically measure some percentage of the machines, then you would feel that you would go forward after meeting that particular threshold. Is that correct?

Mr. DAMSCHRODER. Yes. And then there is an important, I think, distinction, I mean, a recount as we conducted it in the case of the 15th congressional district election last year was statutorily required function to come up with to basically essentially re-examine every ballot that was cast, basically recanvass in the election.

For us in the previous voluntary audits, those were not mandated by law and didn't have the force of a canvass or a vote-certifying function. It was an examination of the paper records to determine the veracity and validity of the electronic results, which in

the case of the 15th congressional district we found that not one vote changed as a result of the examination of the paper trail to the electronic. The only votes that changed were during the hand tally of and the recount of the optically scanned paper ballots.

Mr. GONZALEZ. Yes, sir. Absent a paper trail, how would you conduct an audit? In other words, it lends an important tool. The paper trail is—I guess what I am really getting at, even if you look in Texas in my county, Barrett County, we don't have a paper trail. So if you want to conduct an audit, you are going to have to do it absent that threshold test that you have already described so——

Mr. DAMSCHRODER. And in Franklin County, we had used paperless DREs since 1992. In the case of the 15th congressional district, both of the candidates had been elected and reelected multiple times for different offices using that paperless system.

That is, frankly, why I believe in the voter verified paper audit trail, and supported it in Ohio in 2004 was that I believed that it was important to have a permanent independent record from the electronics who audit the electronic—the electronic record. In the past, recounts have been conducted simply by rereading the electronic results from the electronic cartridges from the voting machines. So by having this permanent paper record that was voter verified independent of the electronic record, we have something to audit the electronic record with.

Mr. GONZALEZ. The other question I think you had posed at the outset of your testimony was something what constitutes a vote, and I am just thinking in terms of I go in there, I vote, I hit the key, whatever, it is registering internally, I am going to be able to read it, but it is also printed out but I am going to need both components in order to constitute the vote. Is that correct? The actual recording by the machine itself internally, electronically but also then the manual printout, the paper trail.

Mr. DAMSCHRODER. Under Ohio law, and under, based on my understanding of this legislation, the paper is the official ballot of record for purposes of the recount. It is my view that the paper record should be used to audit the electronic and that the voter, you know, has cast their ballot electronically, they have saw it in the electronic, but they saw it on the paper, but as I said, it does introduce a new voter intent question that is wildly open to litigation by simply saying the paper is the ballot of record, and giving election officials no guidance on whether to count what appears on the paper as a jam or what does not appear in the event of a blank tape. Those issues—if the paper is going to be used as a ballot of record, States must give local election officials guidance on what constitutes a vote. It is the same issue we ran into in Florida and other jurisdictions with punch cards same issue a lot of jurisdictions wrestle with in optical scan.

Mr. GONZALEZ. My time is just about up.

Mr. Sancho, quickly, you said your preference would be the optical scanner where someone actually marks the ballot and then it is read electronically and such but you still have that, is that correct?

Mr. SANCHO. Yes, it is, and I really think that right now it is the most auditable kind of election. I sort of come back at this from the way of audits. I am—the reason that voter verification even began

was the introduction of the touch screen voting machines which were not transparent and auditable under any circumstances to begin with.

So the idea was to produce a piece of paper that the voters could look at to give them the level of confidence that the machine was, in fact, recording that.

Now the issue is, I like the direction that the Holt bill is discussing in saying that that piece of paper has to be durable. One of the reasons that election officials all across the country are just not very happy with the current technology is that the thermal printers tear and jam. Whether you look at the report emerging out of Cuyahoga County in May, where 10 percent, or even leaving that jurisdiction aside and going to Charlotte—excuse me, Mecklenburg County in North Carolina, where on Election Day, I have—I received their copy of all the Election Day problems. Over 58 percent of all of the reported election problems were on that printer.

The Holt bill says that if you are going to use a paper that comes out of a DRE, that has to be durable, it can't be the these toilet paper thermal rolls. In other words, what they have done is they have established what needs to be audited and left it to the industry to do that. And I will tell that you in the Senate hearing that I was at this week, in Florida, I was approached by my vendor, who told me they have new equipment under development designed to meet that Holt standard, and I was very, very pleased because these thermal papers are awful.

Ms. LOFGREN. Thank you. And the chairman—ranking member of the full committee, Mr. Ehlers.

Mr. EHLERS. Thank you Madam Chair and, I thank you for holding this hearing.

I just want to mention, first of all, that we held two hearings on this topic last year, and I hope that will continue to be part of the record as we review the whole issue.

Ms. LOFGREN. Certainly.

Mr. EHLERS. First of all, Mr. Sancho, I am very pleased to meet you because I am a physicist, and I have been working on ions most of my life. It is really a pleasure to meet one face to face finally.

Mr. SANCHO. And I am a charged particle.

Mr. EHLERS. You look like it.

I have been in this voting business since the early 1970s, and initially not as a candidate, but as working with other elections. I have watched with interest the attitudes developing about the bill that Mr. Holt has offered.

I am not opposed to the bill in principle. I am opposed to some of the specifics in the bill. I think it is important that we have some method of auditing, as both of you said.

Let me first say precisely what my standard is, to start with, I believe that every voter should have complete assurance that the vote they cast will be counted accurately and completely. That is number one.

There is a second part here, which I haven't heard mentioned at all, and that is the voter also has to have the assurance that their vote is not diluted by others casting fraudulent votes or some manipulation of the votes which introduces fraud. Now, I haven't

heard you mention fraud at all. To me, that is a very important factor. When you look back at the history of it, originally everyone had paper ballots. But the reason that voting machines were developed and put in metropolitan areas is to avoid fraud because there was so much shuffling of the paper. Once you have paper ballots, people can hide them, destroy some, ballot boxes can mysteriously appear that were overlooked earlier, questionable marks, et cetera. So I think it is very important to look at both aspects of that as we consider this bill and the problems that arise.

The other problem is, you both mention optical scan ballots, which are used in my home community as well. Again, a paper trail, I am adamantly opposed that the Congress would require that you absolutely have to take one of the options and say that is the official record. I think it should be left to local and State election officials to decide on site which record is more accurate more reliable when they make their decisions.

A good example is during the last presidential election, optical scanned ballots were used in Los Angeles County. There were 30—over 3,600 ballots cast for President in which voters blackened off the ovals for 8 of the 9 candidates and did not blacken that one for President Bush. Now, how do you interpret that? Does this mean that they were blackening out all the others because they wanted to get rid of them but they really wanted to vote for President Bush? Or were they saying, anyone but Bush. In other words, I will vote for eight people, but I don't want to vote for President Bush.

So you can have errors with the paper ballots, too. I don't know how the machine would read them, but the advantage of an electronic machine is that it spots the error immediately and tells the voter, you cannot do that. So we have to recognize, it is one of the big advantages of electronic machines.

So I think it would be a bad error to say, well, it is paper and paper only that counts.

I think it is extremely important that we set good standards. One or both of you mentioned that. If we are going to go to that system I think we have to take the time for the National Institute of Standards and Technology to once again set the standards and make certain that the firms that check these machines are doing it accurately. I think that is a weak link in what we did the last time. We did not empower the standards community to watch the companies that are testing the equipment. So that is something that should be included as well.

So with that, I don't have any questions. I really appreciate your experience. Much of what you say fits together. Some of you have different views on some things but the basic idea is to use an electronic machine, a properly designed one for voting and recording the vote. Use some alternative verification. I would like to talk about 2 reproducible paths. It could be 2 computers frankly. I know computers. I could easily design a system where you have one computer that people vote on.

You have an alternate computer that looks at the same key strokes, analyzes them, records them in a separate fashion, and then you can electronically compare the two. Or you can have a computer and a paper ballot, whether it is optical scan or a tape

or whatever. But absolutely I am unalterably opposed to us in the Congress saying we know what is best for you people, and you have to use the paper trail as a final one, or you have to use the computer. I think the local officials, who have a much better wisdom than the Congress in deciding which one it should be. So I have no questions. Thank you very much.

Ms. LOFGREN. Thank you very much and, we have my colleague from California, Mrs. Davis from San Diego.

Mrs. DAVIS. I wonder if we can talk about a few of the basics, because I don't quite know this. You mentioned the number of hours that were required, just cost generally, how do we look at this? This shouldn't be the biggest factor involved at all, but how expensive is it actually to audit and does that end up playing a role in terms of what counties do sometimes?

Mr. DAMSCHRODER. Well, in Franklin County in the recount that we did to get just 10 percent of the votes from one Federal contest out of, if you look at 2008, we will have 5 Federal contests on our ballot, it took us 2,000 person-hours over the course of several days to do just that one Federal contest.

If we were to do all five—and again, depending on the percentage that we are auditing to, it would obviously take far more than that. The costs for us to prepare and to conduct that—that recount just in terms of overtime alone was $50,000 just for that time frame.

So I view it as a significant cost. If the Federal Government is to going to mandate that local jurisdictions on top of their other election responsibilities and canvassing and verifying provisional ballots and all of the rest to come up with a certified election result, that that poses a significant burden financially on local jurisdictions.

Mrs. DAVIS. Did you want to comment on that?

Mr. SANCHO. Again, since we don't routinely do recounts, and the last one we did was 2000, legally, the issue of how many bodies that we have to hire, what we did was we brought in—it is after the election. We brought in all of our precinct chairmen. So we brought in—we had 150 additional people who we have trained over the course of several years. And we were able to do our portion of the recount within a day in the presidential election.

So again, if you are well organized, if—and again Leon County is not the size of Cuyahoga, we are 150,000 voters, not a million voters——

Mrs. DAVIS. I understand.

Mr. SANCHO. But the issue in Florida is what has it cost us in not verifying our elections, and I would want to say you don't want to pay that cost if you are an election official or a voter.

Mrs. DAVIS. Could you talk a little about absentee ballots and how they are integrated into the ballot?

Mr. SANCHO. They are all optically scanned. And that is one of the things—and Congressman Ehlers made an excellent point. You are going to have problems with any system. Voter education is top of my list of where you must make an expenditure. Voter education is how you interact with the citizens and correctly inform of them of what the possible pitfalls are and inform them over and over and over again how to do this right. If you are not going—if you are not willing to put money into voter education, I don't care what

technology you introduce, you are going to introduce problems with new technology.

So voter education has to be considered excellent money spent up front. The transition from any technology to another one makes that more critical. And that is not where you make shortcuts.

Mrs. DAVIS. Where you have two technologies, or three in some cases, because you have absentee ballots coming in though, is there some things as we consider the importance of the audit that should be discussed?

Mr. DAMSCHRODER. Yes, Congresswoman, and I think, in fact, that is why it is so important that many of the provisions that this legislation seeks to Federalize are handled at the State level. In Ohio, we have 88 different counties. And there are, if I remember correctly, three different voting systems and nine different combinations of those voting systems being used in each of the counties, depending on, for instance, our county uses all touch screens in the precinct, but by mail, absentee ballots are on optical scanned paper ballots.

So when we are doing those recounts, we have to have separate procedures and guidelines on how we conduct each of those recounts or audits. I think—back to your previous question about the cost. I think one of the additional costs that this legislation imposes is the requirement of using auditors with auditing backgrounds, as Mr. Sancho says, he uses poll workers. We used a lot of our staff and poll workers as well. None of those individuals have professional auditing backgrounds or experience that would qualify under the requirements of this Federal legislation. That would again raise the cost of obtaining those people.

Mrs. DAVIS. This is somewhat controversial, perhaps, but the issue of people waiting in line and we all know that certainly plays a factor in the ability of people to stand in line with children in the rain, and terrible situations happen.

Is it worthwhile to look at this issue in terms of a time factor? Is this just a matter of people you know being negligent about not having enough machines for people to use? Where does that issue play into this discussion?

Mr. DAMSCHRODER. I think it is an important issue. But it is one that can't be looked at in a vacuum by just looking at just one of many different factors. The length of the ballot, the length of the language on the individual issues, all of those play into the part of the issue the time it takes. Different States' requirements, some require ID, some don't. All of these different factors, including the number of the extent of the equipment, the number of machines, all of those play a factor in the time it takes for an individual from the time it takes to park the car to the time they return, I don't think you can—it is an issue that has to be examined, but I don't think it is an issue yet that is ripe for legislation, but I don't think all the facets are properly studied.

Mr. SANCHO. I have a little different view on this. Coming into this as an aggrieved citizen who saw the system melt down my orientation is from the voter's perspective. We built our precinct voter system and technology around a voter never having to wait longer than 20 minutes to vote, period. That is the commitment that we make to the voters, we built the number of precincts, and the opti-

cal scan voting system actually is a faster voting system than using, certainly, an audio-based touch screen.

And we have successfully, since 1992, been able to carry out that have responsibility of nobody waiting more than 20 minutes. And when I see lines of citizens waiting four and 5 hours to vote, I am outraged. I personally, would like to see it a crime for citizens to be turned away from the poll without being allowed to vote. To me, my role as the gatekeeper of democracy imposes on my position the requirement that I do what I must to ensure that that gate is not closed on the voter.

Ms. LOFGREN. The time has expired, and we have been joined by the author of the bill, not a member of the committee, and I would ask unanimous consent could to allow Mr. Holt to participate in the questioning for as long as he is able to be here. You are next if you want to ask a question, Rush.

Mr. HOLT. I have just one brief comment. As I came in, I heard some discussion about auditing. And then I also heard a brief comment about waiting times. With regard to the particular legislation that is under consideration here, the idea of an independent board to oversee the procedures of the audit, it does not require that they all be professional auditors. In fact, election poll workers might qualify. It is just that it should be overseen by a person in the State who has that independence from the election procedure. And that is the point, to establish some measure of independence.

With regard to waiting time, I would say that is the subject of other legislation that I've introduced or that others have introduced that I think is worthy of consideration, but probably at another time. Thank you.

[The statement of Mr. Holt follows:]

Statement of Representative Rush Holt

To the Elections Subcommittee of the Committee on House Administration

Hearing on "Auditing Federal Elections"

March 20, 2007

Chairwoman Lofgren, Ranking Member McCarthy, Members of the Committee, thank you for holding this very important hearing, and for allowing me to address the Committee today. Over the course of the years that I have been working on legislation to address security concerns pertaining to computerized voting machines, almost all of the discussion about the bill has been focused on its requirement for a voter-verified paper ballot for every vote cast. But it is not that requirement that constitutes the heart of the legislation – because paper ballots in and of themselves are of no more value to the user than would be a seat belt left unfastened. The heart of the legislation is the requirement that the paper ballots be *used* – used to check the accuracy of the results reported by the electronic equipment. The heart of the legislation is the audit requirement.

Voting is the cornerstone of democracy, and our votes are the single-most valuable component of that process. Everything of value must be auditable. We demand it of our banking, our purchases, and an endless number of other transactions we undertake in our lives. The same must absolutely also be true of our votes. We must put an end, right now, to privatized vote counts conducted on trade-secret protected software and on voting machines that neither produce nor use an independent set of voter-verified paper ballots to check the results.

Some have argued that there has never been a single proven instance of fraud on an electronic voting machine. To which I respond – "how do you know?" If you could independently audit the voting machine, you could discover whether there had or had not been fraud, but it is not possible to independently audit voting systems that have no independent set of voter verified paper ballots for every vote cast. Thus, it is a very convenient argument: knowing full well that there is no evidence available by which to discover or prove fraud, these naysayers argue that there has been no proof of fraud. There certainly are plenty of examples of unresolved questions remaining over election results – questions that will not and cannot be resolved without auditable mechanisms and actual audits.

Thus about 200 of us have legislation pending, the Voter Confidence and Increased Accessibility Act (H.R. 811), that would call for a voter-verified paper ballot for every vote cast, and would put those ballots to their intended use: routine random independent audits of the electronic tallies by hand count of the voter-verified paper ballots in a percentage of randomly-selected precincts in every single federal election. The legislation had the support of a bipartisan majority when the previous session ended, and it has almost that much bipartisan support already in this Congress, after little more than a month following its introduction. Its fundamental requirements – a voter verified paper ballot for every vote cast and routine random audits – have been endorsed by the bipartisan Carter Baker Commission on Federal Election Reform, the National League of Women Voters, the Brennan Center for Justice New York University School of Law, and dozens of public interest and electronic voting integrity groups.

The audit language in the bill is the strongest it has ever been, and I thank Larry Norden and the Brennan Center for conducting an in-depth study into the matter of auditing federal elections, and Candice Hoke of Cleveland State University's Center for Election Integrity and others for contributing their valuable insights to that endeavor. The culmination of the efforts of the Brennan Center audit team is incorporated into the bill, and it will establish a national standard for robust and comprehensive audits in every federal election. At least 3% of the precincts in every federal election will be audited, and in close races, at least 5% or 10% of the precincts. In addition, the critical component of "independence" in the audit, which the U.S. Comptroller General's *Government Accounting Standards* demands, is borne out by giving oversight of the audit process to an independent state audit board rather than to the chief state election official.

After two controversial Presidential elections in a row, and a Congressional race decided by 369 votes being left in utter limbo due to the complete lack of evidence as to what became of 18,000 missing votes, its time to do an about face. We must make every election for federal office independently auditable through the requirement of a voter-verified paper ballot for every vote cast, and we must independently audit every election for federal office, and we must implement those requirements before the next general election.

I thank the Subcommittee again for holding this critical hearing, and I look forward to working with the Subcommittee and the full Committee to bring my legislation on this the topic to the Floor of the House of Representatives for a vote as soon as possible.

Ms. LOFGREN. Thank you, and welcome and thanks to this panel. We keep the record open for additional questions for 5 days, so there may be additional questions to either one of you, and we appreciate so much your taking your time to share your experiences with us as we look at this important piece of legislation. So thank you very much and we will ask that next panel to come forward.

Welcome to all of you. I was mentioning earlier as soon as we notice a hearing, votes are called so we always start these hearings late. So we will ask therefore that you summarize your written statements in 5 minutes. When the yellow light goes on, it means you have about a minute left to summarize. And your full statements will be made part of the official record.

I would like to introduce, in order, Candice Hoke, who is a professor, a law professor, a nationally recognized and widely cited expert on constitutional federalism and major Federal regulatory programs in the context of election law. She is a graduate of Yale law school, former judicial clerk on U.S. Court of Appeals in the first district and a former staff member of the North Carolina governor's office. She leads the center for election integrity as its director and had been appointed as a member of the three-person Cuyahoga election review panel.

Mr. Doug Lewis is executive director of the National Association of Election Officials. He has been the executive director of the National Association of Election Officials since 1994. Also a 501 C–3 organization known as the Election Center. He developed the professional education program, extensive training program for elections and registration officials which awards the certified elections registration administrators certificate upon completion of the program along with other honors and activities.

Lawrence Norden is the counsel for the Brennan Center for Justice, a think tank and Public Law Institute at New York University School of law. He works in the areas of voting technology, voting rights and government accountability and is the lead author of several books relating to machines and voting systems.

He is a graduate of the University of Chicago and the NYU School of Law.

Tammy Patrick is a Federal compliance officer of Maricopa County, Arizona elections department, and is responsible for the recent expansion of the Maricopa County Elections Voter Assistance and Board Worker Enhancement Training Program, which won the National Association of Counties Achievement Award in 2005 and 2006 and is tasked with ensuring compliance with the Voting Rights Act, the Americans with Disabilities Act, and HAVA. Ms. Patrick collaborates with community organizations and voter empowerment groups.

And finally, Pamela Smith, who is the president of Verified Voter and Verified Voting Dot Org, and Verified Voting Foundation. She provides information and public testimony on verified voting issues on State and local levels and has testified before Maryland's legislature, California's Secretary of State's voting system and procedures panel, the San Diego county board of supervisors among others. She has co-authored written testimony on several voting systems and has made legislative recommendations and reports on accessibility and audibility issues for voting systems and other re-

search, and she has been a small business and marketing consultant for many years originally from Chicago Illinois. She is now a resident of Carlsbad, California.

STATEMENTS OF CANDICE HOKE, DIRECTOR, CLEVELAND STATE UNIVERSITY CENTER FOR ELECTION INTEGRITY; R. DOUG LEWIS, EXECUTIVE DIRECTOR, NATIONAL ASSOCIATION OF ELECTION OFFICIALS; LAWRENCE NORDEN, COUNSEL, BRENNAN CENTER FOR JUSTICE; TAMMY PATRICK, FEDERAL COMPLIANCE OFFICER, MARICOPA COUNTY ELECTIONS DEPARTMENT; AND PAMELA SMITH, PRESIDENT, VERIFIED VOTER

Ms. LOFGREN. So welcome to all of you. And if we may begin with Ms. Hoke and move forward for all of your statements.

STATEMENT OF CANDICE HOKE

Ms. HOKE. Good afternoon, Chairwoman Lofgren, Ranking Member McCarthy and Committee members. Thank you for inviting the Center for Election Integrity of Cleveland State University to participate in this hearing on Federal Election Auditing. Since 2006, our Center has held the appointment as Public Monitor of Cuyahoga County Election Reform.

In October, we initiated and obtained Cuyahoga Board of Elections approval to conduct an unprecedented Collaborative Public Audit of the November 2006 General Election. This independent audit was conducted jointly by the County Democratic party, the County Republican party and three election reform organizations. Professional auditors were participants in its planning and execution.

Our Center may be somewhat unusual in that we have been guided by a principled commitment to Federalism as the basis of our election systems. My own scholarly and consulting background prior to undertaking work in election reform focused on the 10th Amendment and Supremacy Clause. In the mid-1990s, for instance, the U.S. Senate's Judiciary Committee, Subcommittee on the Constitution, enlisted me to work on legislation to stem Federal preemption of State law.

I have not advocated Federal legislation as the solution to all electoral administrative problems and don't believe it alone can cure the inadequacies present today. But even as a strong proponent of State powers and Federalism, I would urge that Federal election legislation plays a critical, though as yet, underutilized role in achieving quality elections throughout the Nations. The election system can become a prime example of cooperative Federalism.

Given the expertise present to discuss election audits today, I would like to address only 2 issues in oral testimony: first, the importance of requiring independence of the election auditing structure from the election officials; and secondly, the need to ensure that essential administrative duties for achieving valid trustworthy Federal election audits will be fulfilled.

First on independence: to achieve voter confidence that all valid ballots were counted and counted accurately, the auditors' inde-

pendence from the election officials and the system responsible for conducting the election is imperative.

As my written testimony details, independence is critical for a number of reasons that have been documented in a variety of studies including the SEC's own work on auditing.

Any federally mandated auditing process that does not include true independence will waste taxpayers' time and money and will likely retard rather than augment voter confidence.

Turning to the second recommendation that we made in our written testimony, we would ask that you ensure that the essential administrative tasks for achieving valid trustworthy Federal election audits will be fulfilled. In Cuyahoga County, our collaborative audit was constructed so that the audit policy decisions and choices of races to be audited were invested collectively in the participating political parties and advocacy organizations. Our center was to identify the audit materials needed and to work with the Cuyahoga Board of Elections staff to ensure the logistics and the chain of custody of all needed materials.

The Board of Election Board Members unanimously approved the audit process. We expected staff cooperation and few problems. But I was surprised by the number of impediments that were interposed. First, the existing administrative procedures for processing Election Day materials upon arrival in the BOE meant that we had a difficult time securing the materials in a chain of custody. Second, we discovered software design and electronic election data availability issues that we had not anticipated. Third, certain hardware design issues impeded effective audits. And fourth, we found to our chagrin and sadness that there was staff nonperformance or obstructionist conduct that delayed our audit.

My written testimony provides details about the first three of these types of impediments. I would like to focus on the fourth, staff nonperformance or opposition.

In my experience in Cuyahoga County and elsewhere, I found that many election officials approached their jobs with a high commitment to achieving the best possible elections administrative record with a verifiably accurate and legal set of results. But unfortunately, there is a "group 2," or pockets of election officials who have enjoyed historically unchecked, broad discretionary authority over election performance and over reported election results. Members of this second group tend to disfavor public accountability and independent verification of election results, and thus view audits as inimical to their interests.

I see I need to conclude. I would ask that you keep in mind when you develop the Federal approach that we need to have a process articulated preferably through the States' Secretary of State or their chief election officers that will anticipate various kinds of procedures that need to be in place for effective and expeditious election auditing to occur. A State based system of data collection and other procedures must be articulated well in advance of the audits which will also include specified consequences for local officials if they do not perform. Thank you.

Ms. LOFGREN. Thank you.

[The statement of Ms. Hoke follows:]

Cleveland State University
Center for Election Integrity

Committee on House Administration, Subcommittee on Elections

United States House of Representatives

Statement of

Candice Hoke

Director, Center for Election Integrity

March 20, 2007

The Center for Election Integrity of Cleveland State University appreciates the invitation to participate in this Hearing on Federal Election Auditing. Since August 2006, our Center has held the appointment as Public Monitor of Cuyahoga County Election Reform. In October, we initiated and obtained Cuyahoga Board of Election approval to conduct an unprecedented Collaborative Public Audit of the November 2006 General Election. This independent audit was conducted jointly by the county Democratic Party, the county Republican Party, and three election reform organizations. I have also been a part of the Brennan Center's Post-Election Audit Work Group.

I. Center for Election Integrity's Work to Improve Election Administration and Cuyahoga County Elections

The Cleveland State University Center for Election Integrity was founded in early 2005 in a unique partnering of the colleges of law and public administration. Unlike other election law research Centers then existing, our Center's founders perceived that achieving election administrative excellence in Ohio and elsewhere would require expertise blended from both the law and public administration disciplines.

A Partnership of the Cleveland-Marshall College of Law & the Maxine Goodman Levin College of Urban Affairs
Campus Address 1801 Euclid Avenue, LB 229 * *Mailing Address* 2121 Euclid Avenue, LB 138 Cleveland, OH 44115
216.687.2313 *Voice* * 216.687.6881 *Fax* * www.csuohio.edu/ce/

Our Center's expertise has been recognized by a variety of public appointments and contracts. The U.S. Election Assistance Commission awarded the Center one of the HAVA research contracts, specifically the college poll worker recruitment and training study. After the May 2006 primary debacle in Cuyahoga County, our Board of Elections (BOE) appointed me to serve as a member of its three-person study panel to investigate the causes and cures of that highly problematic election. In August 2006, the Center received a joint appointment from the Cuyahoga County BOE and the County Commissioners to serve as Public Monitor of Election Reform in Cuyahoga County through 2008. Under the appointment as Public Monitor, we proposed the structure of the Collaborative Public Audit and have facilitated the audit.

The Center for Election Integrity, a nonpartisan entity, has been dedicated to three interconnected missions: (1) to assist Ohio in becoming a national leader in transparent, legal, efficient and accurate elections by 2008 (an ambitious aspiration, admittedly); (2) to help ensure that all citizens trust that their elections are fair, lawful and accurate; and (3) to undertake scholarly studies and offer recommendations on election administration and legal reform at all levels of government.

In pursuing these missions, our Center has been guided by a principled commitment to federalism as the basis of our elections system. My own scholarly and consulting background prior to undertaking work on election reform issues focused on the Tenth Amendment and Supremacy Clause. In the mid-1990's, for instance, the U.S. Senate's Judiciary Committee, Subcommittee on the Constitution enlisted me to work on legislation to stem federal preemption of State law.

I have not advocated federal legislation as the solution to all electoral administration problems, and indeed, do not believe that federal legislation can cure the vast range of current inadequacies in the electoral system – in Ohio or elsewhere. But even as a strong proponent of State powers and federalism, I would urge that federal election legislation plays a critical though as yet underutilized role in achieving quality elections throughout the nation. The elections system should be a prime example of cooperative federalism. Thus I am very pleased that this Subcommittee is dedicated to improving election performance and reliability via well-grounded federal legislation.

Given the expertise present to discuss election audits today, rather than reiterate valuable overview points on election auditing that Lawrence Norden has offered in his written testimony, I would like to address in depth only three:

1. The importance of requiring *independence* of the election auditing structure;

2. The need to ensure that essential administrative duties for achieving valid, trustworthy federal election audits will be fulfilled; and,

3. The need to add a specific set of questions that federal auditors should answer in each audit report.

II. Center for Election Integrity Recommendations in Detail

Cuyahoga County's experience pioneering election auditing in Ohio has produced some valuable on-the ground lessons about what is needed in order to initiate and conduct an expeditious, high quality audit of a federal election. I would like to share what seems most critical to your task of structuring federal election audits. In doing so, I would stress, however, that I am speaking only as the Center Director of the entity under which the audit was being conducted, and not speaking for the Cuyahoga Collaborative Audit Committee. I would request permission to supplement my testimony with the Committee's final Audit Report so that you may hear their collective views on the impediments to the audit process, and their conclusions and recommendations for reform.

Recommendation 1: Ensure that Federal Election Auditing is *Independent.*

Questions have risen as to whether power and administrative control over federal election auditing should be vested in an independent body or within the State's chief election officer. Two pending bills, the Count Every Vote Act and The Voter Confidence and Increased Accessibility Act, would establish in each State an independent Chief Auditor or independent Audit Board, respectively.[1] Both bills thus endorse the critical need for the independence of the auditing authority. Some Secretaries of State, however, have taken the position that they should be vested with the federal power to conduct audits of federal elections.

This difference of opinion can be characterized as a debate on whether "internal" audits are sufficient, or whether "external" auditing should occur by a body independent of the administrators under whom control of elections is vested. Which approach is most appropriate for election auditing turns on understanding the differing objectives and outcomes of these audit structures.

The Brennan Center's Lawrence Norden has presented in his testimony to the Subcommittee the five core goals that should motivate the design of election auditing: increasing public confidence in the results of an election; deterring fraud against the voting system; detecting large-scale systemic errors; providing feedback that will allow jurisdictions to improve elections and machinery in future years, and confirming to a high level of confidence that a 100% manual recount would not change the outcome of the race.[2] We agree strongly with this statement of election auditing design goals. In order to achieve these five goals, we have concluded, as has Mr. Norden, that the independence of the auditing entity is essential.

Public confidence in the electoral system has not ebbed simply in Cuyahoga County, Ohio or Sarasota, Florida. Surveys show that the voting public nationwide harbors doubts about

[1] H.R. 1381, 110th Cong. § 102 (2007); H.R 811, 110th Cong. § 5 (2007).

[2] Lawrence D. Norden, Statement to the U.S. House of Representatives, Committee on House Administration, Subcommittee on Elections, March 20, 2007 at 2.

the accuracy and reliability of the electronic voting equipment widely in use today. Media coverage of State and local election officials aligning themselves with the voting machine vendors when questions have arisen have only exacerbated the worries. Additionally, a number of jurisdictions have experienced electoral administration problems that sometimes have included non-disclosure of public records or outright misrepresentations of election accountings, for instance, for the number of ballots cast per precinct as compared with the number of voters registering to vote.

Voter confidence in the integrity of our elections is a prerequisite to the effective functioning of our democracy. Participation via voting depends on citizens' beliefs that their votes will be counted. To achieve voter confidence that all valid ballots were counted, and counted accurately, auditors' independence from the election officials conducting the election is required. Federal election audits can be structured so that rigorous examination by competent and objective auditors occurs. If the auditors lack distance from those having power over the conduct of the election, their objectivity will be questioned. And if election auditors are perceived as lacking objectivity or as influenced by conflicts of interest, voters are likely to view an election audit report that contains good news as nothing more than a whitewash. Thus, an election audit conducted without auditor independence from the election administrative apparatus portends the prospect of being viewed as merely a sham. Any such effort will waste taxpayers' time and money, and will retard rather than augment voter confidence.

The other goals of election auditing, especially that of promoting sound feedback needed for the improvement of the elections system, will best be achieved by instituting a "separation of powers" system of checks and balances, if you will, between the election administrative system and the election auditing authority. One does not impugn the integrity of any sitting Secretary of State (SOS) to reach this conclusion any more than one impugns congressional integrity by advocating the continued separation of the federal judiciary from the federal legislative power. Our nation's Framers were wise in perceiving that certain benefits flow from structural separation of powers. It is not a far stretch to suggest that the Secretaries of State may be stimulated to achieve higher standards of election performance and accountability if they know that federal election audits are beyond their scope of control.

One mystique that can confuse policymaking on auditing is the erroneous perception that auditing is merely a mathematical science with no role for judgment. As the Securities and Exchange Commission has admonished, high quality auditing is "not mechanical, but requires numerous subtle judgments."[3] This perception is as equally true for election audits as for financial audits of publicly held corporations. Because judgment is required at numerous junctures throughout the audit process, control over the audit must be vested in an entity that will foster fair and objective judgments – returning us again to the importance of the independence of the auditing entity.

Given the key role of judgment, externally directed independent audits serve the public interest by reducing extraneous factors that might inappropriately influence an auditor's

[3] Securities and Exchange Commission, *Revision of the Commission's Auditor Independence Requirements*, Nov. 21, 2000 *reprinted in* L. CUNNINGHAN, INTRODUCTORY ACCOUNTING, FINANCE AND AUDITING at 405.

judgment. If the auditors were employed by or under the control of the SOS, such factors might include the perception that "good news" should be the primary objective in the audit report. The auditing profession recognizes that, by contrast, to be an effective auditor, each audit must be undertaken with healthy professional skepticism; as the SEC has noted, the auditor "must have the capacity and the willingness to decide issues in an unbiased and objective manner."[4] Obviously, the independence of the auditors is essential if the election audit is to be conducted with integrity according to the norms of the profession and also to be viewed as reliable by the voting public.

Independence rules, then, should be seen as a genre of conflict of interest rules. As the Securities and Exchange Commission has observed, independence rules, like conflict of interest rules, proscribe certain relationships or circumstances, regardless whether a showing can be made that biased behavior inevitably results from the conflict.[5] "The independence rules are preventive both because of the difficulty in proving the link from circumstance to state of mind, . . . and because of the need to act in the public interest and protect [public] confidence before it has been significantly undermined."[6]

Congress should not wait for an even more serious erosion of voter confidence before requiring independence in federal election audits. While "bad news" election audit reports might suggest impartiality and thoroughness to some members of the public despite lack of independence, we should hope that election audit reports will move toward "good news" as improvements occur. Notably, by providing the public with independent audits now, you additionally protect the public's ability to trust when "good news" audit reports are issued. Unless the election audits are truly independent, undoubtedly any audit reports containing "good news" will be undermined by charges that the report cannot be trusted because the auditors lack independence. Or the audit will be assailed as politically or vendor influenced. I cannot identify any supportable reasons for eroding the foundation of legitimacy for election audit reports that contain good news about the election system.

Because many Secretaries of State hold some administrative supervisory power over local elections, auditing under the SOS cannot completely avoid conflicts of interest that are incompatible with rigorous objectivity and full public accountability. Often, the SOS and their local designees selected the voting systems in use. The SOS often has some power to select or supervise the administrators of elections. With these duties and powers, concerns will be raised that the States' chief election officers will not be as vigorous and unflinching in the audit if the conclusions might impugn the SOS's administrative handling of the election.

At least two reasons have been proffered in support of SOS supervised, as opposed to independent, federal election audits: (1) the SOS knows the nuances of elections as opposed to financial institutions, nuances that can make a difference in the conduct of a valid election audit;

---

[4] *Id.* at 397.

[5] *Id.* at 404.

[6] *Id.*

and (2) a separate system of federal auditing would duplicate and undermine the SOS efforts already underway.

Any value that the SOS can bring in the proper structuring and conduct of election audits can be achieved without injuring the independence that is requisite for the validity of the audit. In particular, I would recommend that the Audit Board approach be utilized, but include a new provision that would permit the SOS to send a non-voting representative to participate. The advantages of elections knowledge and coordination with the SOS where needed can thus be achieved without injuring the independence of the auditing entity.

Where an SOS has already initiated election auditing under its own auspices, that effort likely would be classified as an internal audit rather than as an independent external audit. As the auditing profession would counsel, these two types of audits cannot serve as substitutes for one another. Given that federal elections occur only biennially, the federal auditing structure will generally not be activated except in a federal election year. For all other elections conducted in the State, the SOS-defined auditing system, if any, will control election audits. Where an SOS would prefer that the federal government not erect a different auditing structure because it will impliedly cast aspersions on the auditing structure that lacks independence from the election administrative authorities, my hope would be that you rise to the occasion. Specifically, you can teach via federal legislation a better set of norms for election auditing, and implicitly prod the States into adopting independent election auditing as the baseline for their efforts. By no means should your design of federal audit legislation become less effective – as by eliminating independence – simply so that some Secretaries of State will not be embarrassed by the weak audit efforts underway in their States. The federal government should articulate as close to a "gold standard" structure for election auditing as is feasible, and lead the way out of the current election wilderness.

I would thus urge that you adopt an approach similar to that outlined in H.R. 811, section 5 with the possible addition of a representative of the State's chief election officer as a nonvoting representative.

Recommendation 2: Ensure that Essential Administrative Tasks for Achieving Valid, Trustworthy Federal Election Audits Will be Fulfilled

In Cuyahoga County, our Collaborative Audit was constructed so that the audit policy decisions and the choice of races to be audited were vested collectively in the participating political parties and advocacy organizations. The Center for Election Integrity was to identify the audit materials needed and to work with the Cuyahoga Board of Elections to ensure the logistics for the secure chain of custody of all needed materials. In three public Board of Election Meetings prior to the commencement of the audits, the audits had received unanimous support from the Board Members. We expected staff cooperation and few problems. We believed it was a relatively straightforward process.

But I was surprised by the number of impediments that were interposed by:

(1) existing administrative procedures for processing the Election Day materials upon arrival in the BOE;

(2) software design and electronic data availability issues;

(3) hardware design issues; and

(4) staff nonperformance.

Taking each area in turn, here are some examples of difficulties we faced despite dealing with only one local Board of Election:

(1) Existing administrative procedures and storage equipment did not meet the requirements for a secure chain of custody for DRE (voting device) long reports. We had to educate the local officials on the meaning of a "secure chain of custody," identify election night procedures that needed to be modified to reach these standards, ensure that appropriate staffing was available for re-sealing the DRE Long Reports in envelopes, and supervise the Election night placement of the Long Reports envelopes in sealed bins until the audit was authorized to begin two days later.

(2) Software design and electronic data availability issues: Well before Election Day, we identified in writing in clear generic terms exactly what electronic election results data were needed to complete the audit. The Ballot Department staff assured us that this would be provided to us immediately upon the close of the unofficial tabulation. I stayed up over 36 hours to be present when the election closed so as to receive immediately the data files and to protect the chain of custody. Despite these efforts, however, the electronic files proved not to contain the data that we needed for the audit.

In a series of follow-up conversations, the BOE managers (who consulted with their vendor, Diebold Election Systems, Inc.) informed us that no one or two files would have the data that we needed. Instead, they informed us that a variety of files would be required, and that we would have to engage in a series of mathematical steps in order to extract the data that would permit a comparison of the DRE units' and optically scanned ballots as against the central tabulation data.

As a result of the conversations and representations, we ultimately filed a request for eight separate electronic files.[7] To this day, we have no knowledge of whether a far less

[7] GEMS is Diebold's election tabulation software. The eight files we requested after extensive discussions were:

a. GEMS Statement of Votes Cast (SOVC) Report run on the database backup after absentee ballots were tabulated, but *BEFORE* DRE memory cards were uploaded.
b. Database file from after central count optical-scan absentee ballots were uploaded, but before GEMS tabulation was performed.
c. GEMS data export from after absentee ballots were uploaded but before the GEMS tabulation was performed.
d. Database file after DRE uploading was complete.
e. GEMS data export after DRE uploading was complete.
f. GEMS SOVC Report after all absentee ballots performed on DREs.
g. Database file after all absentee ballots performed on DREs were uploaded .

complicated route was available for obtaining the requisite data for the audit, and we have no way to obtain reliable information on this question. We do not know if the information we were given was actually deliberate disinformation by an election department that did not support public verification of election results, and thus gave us a run-around to obstruct the completion of the audit. We lack reliable information on whether Diebold's GEMS software actually does not accumulate and report election data in a manner that easily facilitates an election audit, or whether the Cuyahoga Ballot Department staff handled election tabulations in a manner that obscured the data needed.

(3) Hardware design issues: A little known secret about current generation major brand optical scanners is that they do not count *ballots* but only ballot *pages*. Thus, even if we know the total number of optical scan ballots that the BOE received for tabulation, we have no easy way to determine whether all the ballots were part of the tabulation. In Cuyahoga County, for instance, in the General Election in November, among our 59 separate jurisdictions, ballots were as short as 3 pages or as long as 6. To determine whether all the ballots had been counted, the BOE executives simply averaged the number of ballot pages and *estimated* that all the optical scan ballots had been counted.

By contrast, with punch cards the BOE was able to determine with complete accuracy whether all the ballots that had been received had been counted. The optical scan hardware (and firmware) design, however, does not include features that are essential to determining whether all ballots are counted. So now, as a result of this new, supposedly HAVA-compliant equipment, we have reduced rather than augmented the accuracy and reliability of our elections results. This reduction in reliability apparently owes to a engineering design omission, one that must be redressed via expensive auditing procedures since the equipment opens this cavernous hole in election reliability.

(4) Staff nonperformance or opposition: In my experience in Cuyahoga County and elsewhere, I have found that many elections officials approach their jobs with a high commitment to achieving the best possible elections administrative record, with a verifiably accurate and legal set of results. But unfortunately there is a "group 2" – pockets of election officials who enjoy the historically unchecked, broad discretionary authority they exercise over election performance and reported electoral results. Members of this second group tend to disfavor public accountability and independent verification of election results, and thus view audits as inimical to their interests.

If, as in Cuyahoga County, some "group 2" officials have control over some audit documents or electronic files that are needed to conduct the audit, or the staffing needed to supervise the hand count, the result may be what we experienced: repeated delays and extra costs for completing the audit tasks. And if the executive management is also not enthusiastic about the audit, excuses can continue to pile up for why certain activities cannot be scheduled, or

---

h. GEMS data export after all absentee ballots performed on DREs were uploaded. See the forthcoming Cuyahoga Collaborative Audit Report on the November 2006 Election for further details.

why staff had to cancel at the last minute, or why certain files and documents will not be released for the audit.

I bring these experiences to your Subcommittee because you may have assumed, as did we, that if an audit is formally authorized and directed, then the local or regional election staff will cooperate in fulfilling the federal audit directives. You may expect, as we did, that the requisite election data is already present and (other than conducting some hand counts) would require only some quick comparisons in order to conduct the audits. Neither assumption is necessarily sound. Importantly, cooperative federalism offers solutions that should solve the problems and redound to the benefit of all concerned.

Defining the Key Roles of the Secretaries of State

(1) Mandating Documents and Local Support In light of the obstacles we encountered, the expressed desires of some Secretaries of State to be involved in the audit process, and in the spirit of cooperative federalism, we would recommend that the federal legislation specify that the States' chief election officers should mandate what procedures and information (including data files) elections officials should provide to the auditors.

The mechanism that I would recommend is a conditional preemption approach, which would not implicate Tenth Amendment issues and thus spawn litigation.[8] The federal legislation would thereby offer the SOS a choice: determine and mandate, in light of the election technologies in use in your State currently and any other considerations, what documents, files, procedures, and access and support need to be provided and in what time frame in order to achieve compliance with the federal audit requirements, or, lose the right to determine these directions and have this power vested for the next four years in either (1) the Audit Board, or (2) the U.S. Election Assistance Commission. In fashioning the State directives, the legislation should direct the SOS to consult with the Audit Board. You might also consider conferring an explicit right for the Audit Board to compel recalcitrant SOS action via mandamus if the Board believes it necessary for achieving its charge.

(2) Further investigation and remediation Given the short period of time for achieving remediation if errors are discovered, SOS should specify in advance the protocols for further investigation and remediation of the errors if discrepancies are found.

(3) Training election officials in values of auditing Currently among election officials the movement toward auditing is frequently viewed to be playing a game of "gotcha" – as if auditing were primarily motivated by distrust of the elections officials. At least in Ohio and maybe elsewhere as well, there has been little effort to teach the underlying objectives and values of auditing– especially the five goals that Mr. Norden outlined. This omission in election official training should be rectified by each SOS, although I doubt that it would be wise to mandate the training in federal elections legislation. Perhaps other mechanisms can be identified.

[8] *See New York v. United States*, 505 U.S. 144 (1992).

Administrative planning by the Audit Board or other Audit Entity

In order to be ready to conduct and complete an audit immediately after the unofficial tabulation, a great deal of logistical and other planning will need to be completed well in advance of the election. The Audit protocol should have been determined, and test runs should have occurred. Qualified personnel will need to be identified and retained to conduct the audit. Notice must be provided to the local elections officials concerning the need to plan and provide appropriate staffing. A protocol or format for the audit report should also be established well in advance to allow for quick submission of audit results and any corrections to the certified count procedures.

Recommendation 3: Add a Specific Set of Questions that Federal Auditors should Answer in an Audit Report

Consistent with auditing principles, the federal statutory charge on auditing federal elections should require answers to four standard auditing questions (which can be answered using scientific sampling methodology).

In considering the tabulated and reported election results:

1. Was every valid ballot *counted*?
2. Was every valid ballot counted *only once*?
3. Were the votes recorded on valid ballots *accurately* reflected in the announced totals?
4. Were *more votes* recorded in the totals than those reflected by valid ballots?

Currently, the conceptions for federal audits represented in the Count Every Vote Act and The Voter Confidence and Increased Accessibility Act do not encompass all of these questions. Yet each question is essential in order to determine whether all valid ballots and votes were tabulated and not simply the accuracy of the ballots that have been tabulated. Where an election audit cannot reliably answer one or more of these questions, some administrative procedure or even voting equipment design changes may be needed.

CONCLUSION

Mandatory election audits are a critical step for restoring public confidence in the electoral system and for learning what problems exist (in equipment, systems, and personnel) so that they might be effectively corrected. Unfortunately, the promise of auditing will be severely undermined if the federal auditing entity lacks independence from the election administrative authority. Secretaries of State can play a number of crucial additional roles that will facilitate efficient and effective election audits, but because of the appearance of conflicts of interest should not be supervising and conducting federal audits. The federal audit effort will be greatly enhanced if the legislation will require each audit report to answer the above four key questions.

Ms. LOFGREN. Mr. Lewis.

STATEMENT OF R. DOUG LEWIS

Mr. LEWIS. I obviously cannot cram 8 pages of testimony into 5 minutes, so let me just try to summarize as best I can for you all.

We do a form of audits now. Every jurisdiction in America does a form of audits. It is called canvass the vote, and this is one of those things that—a whole lot of people who are not involved in elections do not understand it, but we go through a process of where we actually do try to reconcile all of the numbers and make sure that the numbers are what the numbers should be; that we go back and look when the numbers do not make sense, and in fact, usually whenever there is a problem with an election, it is because an election official found that the numbers did not make sense somewhere, and then he went back to investigate to find out why.

In terms of whether or not we ought to have an audit that verifies that the equipment is counting correctly, quite frankly, I do not think you are going to find that most election officials disagree with that. It is how it gets done. It is whether or not what you are doing in H.R. 811 actually gets to that and does it in such a prescriptive manner that it really makes it very difficult to do this.

So I would say to you, as Congressional people, rather than trying to tell us exactly how to do each and every one of these things, determine the areas that you want to have policy decisions made in, and instruct us to figure out a way to do that. Tell the States and the locales what the basic standards are that you want to achieve, and then let the laboratory of 7,800 jurisdictions in America go to work. You will find there are several right answers more often than not, and I have been on record as saying that having an audit that proves that voting systems work is not a bad deal. That is a good deal. It is just a matter of how we get there.

The problem, I think, is that if we get this thing so complicated, instead of achieving your goals of higher believability and acceptance of the process, we end up destroying the very thing that you are trying to improve, and so let us make sure that we do not get to the point that we complicate this so much to the point that nobody has faith in it at all. We are at the point where we have got to be careful that we keep beating on the system, alleging that somehow the system is wrong when the system works pretty cotton-picking well. It may not work well in the estimation of some who are very, very partisan in their viewpoint on this (and that is on both sides of the aisle depending on what the issue is) and so it is one of those that we have to look at. If you go to the point of trying to build escalating audits of all of the Federal races and going through counting all of them, you are going to find that humans count far less accurately than equipment does. Every time we go into one of these recounts, every time we even do the audits in the States that actually do these audits, you find that the real problems come from humans, not from the equipment. I mean, we do have some equipment problems on occasion, but it is rare when compared to the problems that humans make, and so it seems to me that where we need to be in this is, do not assume that humans are going to be the better answer for this whole process because, as election officials, we know after recounts and after audits of

doing this, when we find an error, it is usually the humans who have made the error and not the equipment.

In terms of when you look at the costs of all of this, there always is a tendency, I think, of any legislative body, that when it wants something, it always underestimates the cost of what it is going to cost to accomplish the objectives, and it is always easy to shift that cost to somebody else that you are not paying for, to always push that down to the lowest level and say, well, the jurisdictions can pick up that cost.

The problem with all of this is that we have started to make the jurisdictions responsible for all costs and, you must know that they are almost at the breaking point in terms of the cost of election changes. My concern is this: If Congress begins to assume that it knows more about the management of practices of elections and that it knows more about what will work than local governments do, that it wants to be uniform across the United States, then I think democracy is going to be in for a very rough period.

Secondly, in wrapping this up, let me say to you election officials in America are dedicated people. They do this with little money, not a whole lot of support most of the time. They get vilified as somehow people who are manipulating elections when none of that seems to be able to be proven in 99 percent of the cases. It seems to me we need to recognize these are good people trying to do a decent and honest job.

Thank you.

[The statement of Mr. Lewis follows:]

Madam Chair and Representatives:

Thank you for the invitation to appear before you to discuss potential changes in election practices of the states for future federal elections.

I don't purport to speak for the entire elections community nor all of the professional men and women who make this great democracy work so well. I have, however, been in the elections profession long enough to know where the majority of the elections community will fall on most issues of continuing "election reform."

Our concern, those of us who work day in and day out, to make this process work well for voters and work well for candidates and political parties, is that you use considered judgment when contemplating additional changes in this process.

Audits of Elections. I was invited here to talk about both the concept of an audit process as applied to elections and to talk about potential legislation to affect US elections.

Let's tackle the audit process first and then address the broader concerns.

Audits of elections is not a bad concept. I have said publicly that I personally have no problem with it as long as everyone understands that it lengthens the time to close an election and it adds significantly to the cost of doing the election. Finding out if your equipment is counting accurately or your people are counting accurately is not something you will find troublesome to elections professionals...as long as there is time provided in the process to do this.

So often it is said the "The Devil is in the details." The Devil is not just in the details, it is often in the definitions. What is an audit? Are we all agreed as to what is meant by the term audit? And do you do the audit as a matter of common practice or when questions are raised or when there is a close election? It makes a difference in cost structure and perceived value for the taxpayers paying for it.

Types of "Audits". Canvass Audits. For many election officials, the term "canvass the vote" is an audit and by that definition every election jurisdiction in America conducts a form of an audit. The canvass is to assure the numbers check against those who showed up in the precincts, looking at the number of ballots distributed, those retained as unvoted, the number returned, the number voted, that the totals are the same as those filled out in the official reports and if there are discrepancies, to get those reconciled. Canvass audits occur at both the local and state levels to check and recheck numbers to be sure the "official" vote totals are then reported. And you should know the election canvass/audit that currently occurs prior to certification of official results is a transparent process open to public observation.

Recounts as Audits. An audit is also a result of a recount and often in a contested election (these are two separate conditions in election terminology). In a recount, a race has to be close enough to

warrant handling the ballots again. But it is also examining the ballots by hand to assure that the equipment has counted legitimate votes and anything a machine can't count is usually processed separately and reexamined by humans to see if they can determine the problem. In the case of electronic voting, voters can rarely make errors on the equipment and there is little to recount. In the case of paper ballots processed by optical scan devices or by hand, voters can and do make substantial errors that may or may not be read by the device. If the optical scan equipment can't count a ballot or can't count a race on a ballot it can be "kicked out" and then reviewed by humans.

In the minds of many, a recount is the most effective audit of all. It is done only when there is a sufficient reason to do so. Therefore it is not an ongoing cost of conducting elections for the jurisdictions when there is no close election. Likewise, a contested election might also be required in a judicial process to recount ballots.

Audits of Voting Equipment. There is the concept of an audit to assure that the votes as counted by the voting equipment are accurate. In this instance you want to do enough to make sure that you have a confidence level that says there is nothing wrong and you proceed with the machine count. To establish a random process and to have that process work does not require ever increasing percentages of ballots to be counted however. If it is designed correctly and it is a "random" audit and is a uniform process throughout, then the audit can be performed one time for all races or a selection of races to show that the hand count matches the machine count.

But there is the rub. Humans count large numbers of ballots less accurately than voting equipment does. The higher you establish the "required" percentage to be counted the more you will find discrepancies ... and those discrepancies are rarely the voting equipment's numbers. It is because humans either make a mistake in counting or because a human interprets a ballot differently than the equipment. Humans get tired. Their minds wander when counting large numbers of ballots by hand. Even the same person counting ballots over a long period may count ballots differently during the early part of the audit process than the later part of the process because of mental and visual fatigue. Greater percentages require more and more people. And because of the potential for more mistakes, it forces additional counts to resolve the differences caused by human error.

Audits by Outside Agencies. HR811 calls for audits by State Auditors or by appointments through the AG of the state and not by election officials. We want to be kind here, but this may be the worst of the ideas that have been offered in election legislation. Under these provisions, you turn the process of live ballots over to people who have no idea of what goes into protecting those ballots, who have no experience in assuring the protection of the voters' votes, and who will be handling the ballots without the training of what to look for or what to do if there are problems with the ballots. Additionally, they are doing audits that then impact the "official" record of the votes. Name an election official in America who wants to be responsible for ballots that have not remained in their possession.

Congress also has to address these concerns: in the case of a court proceeding or an imposed recount, who has control of the ballots? The election official or the outside auditors? If the outside

agencies do this work, they will bill someone for the work. Is that to be local governments who pay the bill? Or state governments? Is Congress going to provide continuing funding to pay for these?

Additionally, election officials are trained to be neutral when processing votes in an election. We train our staff and our counting teams that we are protecting the ballots as the voters voted them. The process described in HR811 turns the auditing process, on which we must base the results, over to partisan offices. Having ANY non-election official responsible for handling live ballots is an incredibly bad idea. This is where the nation is best served by the professionalism and neutrality of election officials. If Congress wants to provide for outside observers of an audit process while in the hands of election officials, that is an acceptable and workable alternative, but we implore you to discard this notion of letting others handle live ballots. The temptations and opportunity for chicanery and possible manipulation of votes is too great a danger to attempt. Election officials are trained and live to the standards necessary to assure that the election is an accurate reflection of the public's will.

We know that when policy makers want changes that costs are rarely a genuine consideration. But in good conscience we must warn that audits by elections agencies will be more expensive in virtually every state and local jurisdiction in the nation. But to have outside audits done will be exponentially more expensive and someone other than local jurisdictions needs to bear the brunt of this and the other changes in HR811. This will become a huge unfunded mandate on local governments and even in the best of circumstances it will be a massively under funded mandate.

Additional Problems Caused by Outside Audits. Congress must understand that the kinds and numbers of audits specified in HR811 have the potential to drag an election past reasonableness – or to cause a Presidential election to end up before the Supreme Court again. The audits, and the requirements of them as prescribed in the legislation, have the potential to affect the time for a recount of an election beyond the period that the Electoral College must meet to determine the winner. What we learned in Election 2000 is that the current schedule is not sufficient for a real recount of a Presidential election. While states can attempt to shorten their canvass process to get more time for a recount, there is unlikely to be sufficient time with the audit process specified in HR811. And when that happens the courts become the recourse.

Simplify: Set Objectives, Not Administrative Methods

The process described in HR811 is unworkable and unnecessary. Simplify.

If an audit process is necessary and desirable -- and almost 70 percent of the states have not felt compelled to do an audit as it is being considered in legislation -- and if Congress wants to establish an audit process, then it needs to let the states and local governments figure out how best to do that. Simply tell the states that an audit process is required. Then back away and let them figure out how to do it best to serve their voters. The audits currently conducted by states range from states that randomly select a number of precincts and then reprocess the ballots in those precincts and chose

races on which to do that, to the kind of audit done in California where the audit is one percent of all precincts and all races within the precinct.

But to run multiple audits at the same time for different races with different requirements as specified in HR811 is a nightmare that will have the opposite effect from the one intended. At some point you have to end the election. Voters need to know and want to know the results. And if elections offices are still doing multiple audits 30 days or later before they can report official vote totals, the public will begin to think the election is being manipulated in the interim. Additionally, candidates want immediate results and don't want to understand imposed delays – almost all of which are the result of legislation.

When anything gets too complicated, it breaks more often. Be careful here. Go after the objective if you want, but dump the prescriptive methodology. If the objective is more confidence in elections, then don't create a situation that is more than likely to lead to less confidence.

Problems with Audits of DREs with paper ballots. If the audit called for in HR811 is to include paper records produced by DRE (electronic) voting equipment, then be prepared to wait much longer times to finish an audit. So far every jurisdiction that has tried to audit or recount paper records produced by DRE's, and has to do so with humans instead of technology, the counts are taking exponentially longer times to complete than any other form of voting. Please know that as election officials we have been, and continue to be, seriously concerned about audits and/or recounts of paper ballots produced by DREs. This is far more difficult than is being acknowledged and is a slow, grinding process. The solutions for this are not yet sufficient and the design of the systems is not yet conducive to making this a quick process.

We tend to forget why we moved to voting equipment. It is more accurate. It is more difficult to manipulate – despite the allegations to the contrary. It counts faster. Machines make few errors, humans make many.

Realistic Timetables: Trying to implement these provisions by 2008 will be unrealistic. The changes required through HR811 are major feats and taken separately, if Congress were to specify these kinds of objectives, the implementation deadlines need to be realistic. We take a real risk in trying to make changes of a major nature in a Presidential election cycle. Your colleagues in previous Congresses on HAVA did not push for 2004 because they knew they put the election process in danger by doing so and instead ordered all changes by 2006 so the jurisdictions could have practice before the Presidential election of 2008. If any one of these objectives is key, then let that first one be implemented by 2010 and then stagger any other changes to occur in elections beyond 2012.

Clearly we still have states that are struggling to meet the requirements of HAVA and it is not because they have been unwilling to comply. It simply takes more time that HAVA allowed – and we warned Congress then that some of the expectations of timelines were too aggressive for the conduct of elections to high standards that are required in US elections.

Other Concerns About HR811

Security Issues: As to other parts of HR811, our message to you is this: if you want to achieve voting systems security, this is probably not the right answer. You can better accomplish that task by instructing the US Election Assistance Commission (EAC) to work with the National Institute of Standards and Technology (NIST) and tell them to develop methods for assuring security of voting systems and election software.

Paper Records on DREs: If the objective is truly to force paper into the voting process regardless of the technology, then HR811 is not the way to do that. When discussing the requirements for DREs to have paper, it is my understanding from my colleagues around the nation there is no state yet which could comply with the paper trail system as specified in HR811. So the 27 states that have previously taken action would have to scrap what they have already done and spend hundreds of millions of dollars to revamp once again. Surely this Congress does not intend for that to happen. And what could they buy if they wanted to continue with DREs? From what we're told, nothing currently manufactured as a DRE can comply.

Other Election Reforms Require Use of DREs: Congressional leaders have introduced legislation that includes an "election reform wish list" of changes to be accomplished -- such as every state conducting early in-person voting and a greater expansion of the Vote Center or Super Precinct concept -- that cannot be accomplished in urban areas without safe and secure DREs. What objectives does this Congress have in relation to these stated goals and how is it to achieve them? Some of these cannot be accomplished with Optical Scan or hand voted paper ballot systems.

Confidence of Voters. If confidence in the process was lost as a result of Election 2000, then it had fully returned by Election 2006. Yes, there were some problems in a relatively small number of places in the more than 7,800 jurisdictions that work with federal and state elections. And some of those problems were "doozies". But remember, those problems were the exceptions in 2006, not the norm.

Elections in 98.6% of the jurisdictions in America worked exactly as intended, and served voters and served candidates and served democracy exceedingly well.

But we are continuously told in some quarters that there is a "crisis of confidence" for voters. Polls conducted in 2006 immediately after the election say that allegation simply does not stand up. If there was a crisis in voter confidence, then why did 88% of the voters tell CNN in exit polls that they "had full confidence that their vote was counted accurately and fairly in Congressional elections" ?

I have been looking at those confidence numbers for more than 30 years and that number has never been higher than 88%. There are and have been segments of our society who do not have the same kind of faith in voting but the overwhelming majority of actual real voters clearly tell us they have confidence in American democracy.

And, the process must work pretty well. Each of you serving in this Congress got elected by this process. It must have been fair and honest and open, or we would still be in courts throughout the land fighting about what happened.

What is interesting to contemplate is if the process is working, and it is, and if the public has overwhelming confidence in it, and it does, then should we be in a rush to make additional and invasive changes?

The reason that it took almost two years to fashion and pass the Help America Vote Act was that Congress became aware of the complexity of the process and wanted its actions to do no harm. I trust that this Congress will want to be deliberative in considering the additional proposed changes offered in legislation.

Too Much Change on Top of Massive Change May Break the System. The election process in America has undergone the most massive restructuring in the history of elections in the United States. The passage of the Help America Vote Act made more fundamental and direct changes in the way elections are conducted than at any other time in the last 100 years. Important and needed legislation such as the Civil Rights Act and the Voting Rights Act profoundly changed democracy for the better in America.

But those Acts did not reshape and transform the entire process of election administration in the manner and to the extent that the Help America Vote Act did. Elections in the United States are still digesting the sweeping massive HAVA requirements put on the states and local governments: to this day, many of the states continue working either to establish or perfect statewide voter databases. Many states are still perfecting the provisional voting process mandated for the nation. HAVA established voting requirements for voters with disabilities that allow for independence and privacy as afforded to other voters and we have not yet fully achieved the goals for that mandate. HAVA's goals of dramatically changing the types of voting methodologies and the use of technology different from the technology used over the past 30 to 100 years, forced major voting equipment upgrades for virtually every jurisdiction in America. HAVA gave states far more responsibility for the actual conduct and results of elections than had previously existed and states are still working to build their experience levels for such a significant operational shift from local governments to the state level for many functions.

My point is that we, the nation and the elections community, are still in the process of absorbing a major restructuring and until we get a chance to learn how to perfect all the massive changes, it is dangerous to assume that we can continue to pile major change upon major change and not have it result in seriously damaging unintended consequences.

As a profession, we are used to change. And rather than working with people who always want the "status quo", it has been election officials who have prompted and promoted virtually every election

innovation of the last 50 years. But we believe in "orderly change" so the process serves voters well and that confidence can be maintained.

Our lesson from HAVA is that it left the local jurisdictions "holding the bag" and having to pay substantial increased costs of conducting elections not just in 2004 or 2006 but for every election in the foreseeable future. Yes, HAVA pumped almost $3 billion into the process – much of which will have been wasted if the provisions of HR811 are enacted as written – but it left local jurisdictions with on-going costs that approach almost a third of that during every election cycle.

HR811 Underestimates the Cost of Its Mandates. Why is that important? Because as Congressional representatives, you need to know that additional federal legislation that mandates changes such as those in HR 811 will once again result in changes so massive that it is likely to exceed the amount required for HAVA. You cannot, in good conscience, accept that such changes are limited to $300 million as proposed in the legislation. It is more likely that it will be as much as HAVA – or more – for its short and long term impacts.

Conclusion: The question is not whether we should change elections policy and practices. We can do that from time-to-time and absorb individual changes. But the question has to be is should Congress be the one specifying not only the changes, but the practices, the implementation, and the deadlines?

Establish Objectives, Not Methodologies: A more prudent way to do this is for Congress to establish basic values that it wants the election process to have such as fairness, transparency, auditability, security and what it wants the process to do for voters. If you want security of voting systems, then establish that as the mandate and then let the states and local jurisdictions figure out how best to accomplish that. Don't get prescriptive and establish exactly how that will get done. The genius of the American democracy is that it is so diverse and it proves continuously that there is almost always more than one right answer. It is such a wonderful laboratory that virtually every great advancement in elections has come because the states do this very differently and it creates new ideas such as "early voting" or vote centers. Congress needs to know that virtually all of the major HAVA requirements were based on existing state initiatives such as statewide voter databases and provisional voting.

The role and objective of Congress is to assure Americans that the process serves voters and the democracy well. But if Congress begins to assume that it knows more about the management practices of elections, that it knows more about what will work than the local governments around the nation, that it wants it to be uniform across the United States, then democracy is in for a rough period. We should have it well established by this time that one size or one solution does not work well in all parts of America.

Let States Decide: Regardless of whether you are a liberal or a conservative or somewhere in between, whether you are a Democrat or a Republican, whether you come from a large state or a small state, by now you have heard from your local and state election officials especially since

Election 2000. The people you and your political and governmental colleagues have chosen to administer the process in your home state and home jurisdiction have told you time and again, that the process works best when it can be structured to serve the voters in each state. You can talk with members of your own party who serve in the elections community and they will confirm that as the truth.

Lessons Learned From the Recent Past: We must resist the temptation to assume that those in Washington know best how to administer elections in the 7,800 jurisdictions. If we learned nothing else since Election 2000 we should have learned by now that this is a vibrant but often fragile process. Making this process work well for voters has been continuously evolving during the 231 years of the nation and frankly we have learned lessons that have shaped it well.

Election Officials Have the Same Goals: Finally, please know that election officials are not the enemy. We want what you want. We want voters to have a good experience. We, like you, want the process to be fair, honest, and accurate. We, like you, want it to be transparent. We, like you, want it to work flawlessly. While we strive for perfection, a process that involves 168 million registered voters, 122 million voters who go to the polls at 200,000 polling sites in 7,800 separate jurisdictions, using 800,000 voting devices and employing 1.4 million poll workers is likely to have occasional problems.

But don't assume that the 18,000 professional election officials employed to do this job in America are nameless, faceless bureaucrats. These are decent, caring and dedicated people who take their responsibility to voting, to voters, to democracy and to freedom seriously. They believe in this process. They believe in service to voters. They make the process work even when they are not given adequate resources to do so. They make it work even when some groups and individuals vilify their efforts and their dedication. Listen to their advice. The advice is not born of partisanship but of respect for the dignity of the voters who participate in this great democracy. They are willing to work with you to see that a healthy democracy survives into the next century.

****

The Election Center – The National Association of Election Officials. www.electioncenter.org
The Center is located at 12543 Westella, Suite 100, Houston, TX 77077

The Election Center is a national nonpartisan, nonprofit organization working with the nation's elections administrators to improve the administration of democracy. Its members are the government employees at the township, city, county and state level who are responsible for the conduct of voter registration or election administration. As the largest elections related organization in America, it works with both domestic and international democracies to improve the professionalism of elections and serves as the certification body for the profession for those who earn the status of Certified Election/Registration Administrator (CERA), the nation's highest achievement for those in elections. Doug Lewis, CERA, has served as the Executive Director of The Center since 1994.

Ms. LOFGREN. Thank you very much for your testimony.
Mr. Norden.

STATEMENT OF LAWRENCE NORDEN

Mr. NORDEN. Thank you.

Thank you to the subcommittee for holding a hearing on post-election audits, I think a subject that probably would strike most people as rather boring but that, in fact, is critical if we are going to secure our elections, improve them and restore full public confidence in our electoral system.

My name is Lawrence Norden, and for 18 months, I was chair for the Brennan Center Task Force on Voting System Security. This task force included the Nation's leading computer scientists and security professionals, including scientists from the National Institute of Standards and Technology, and the former chief security officer of Microsoft and former cyber security czar for President George W. Bush.

What the task force found, I think at this point, is a consensus view among security experts and computer scientists who have looked at electronic voting machines, and that is that there are serious security and reliability vulnerabilities in these machines. The good news is that there is also a substantial consensus on how to address these vulnerabilities, and one of the most important things, it is agreed, that we can do is to use post-election audits to compare voter-verified independent records to the electronic tally. Fortunately, this is already happening in many States. As the chair mentioned, Connecticut in the last election audited 20 percent of its precincts that were using optical scan machines. Illinois regularly audits 5 percent of its precincts, and California audits, as many on the subcommittee know, 1 percent of its precincts. It has for a long time. In many cases, this is counting up to 200 races in a single county. Unfortunately, this is not being done in most States, and it is the reason why we need Federal legislation mandating good post-election audits. What would that look like?

The Brennan Center has been working with the University of California at Berkeley's Samuelson Clinic, and with many leading election officials and academics to answer that question, and we will be issuing a report on that subject shortly. I detail many recommendations in my written testimony. I am going to briefly mention a few of them.

The first is that it is crucial that the selection process for audits be random and transparent, and Cuyahoga County, in 2004, is an excellent example of why this is necessary. In 2004, after the general election, election officials were doing a 3-percent post-election audit and pre-sorted the ballots to make sure they matched with the electronic ballots, so the audits showed that the paper and electronic records matched. But this actually was not a check on the system; it did not prove anything. If the process for selecting the machines to be audited were public and it were clear to the public that the selection was random, this is a problem that could have been avoided.

Secondly, we need to increase scrutiny, audit scrutiny, in close elections. In most Federal elections, a 3-percent audit will be sufficient to have confidence that a full recount would not change the

results, but in very close races where just the corruption of a few votes or a mis-tally could change the outcome of an election, a 3-percent audit does not give you, really, any confidence that you will have caught an error that might have occurred. To his credit, Congressman Holt introduced this concept in his legislation.

Third, a good chain of custody is key, and again, the Cuyahoga example is a great example for why this is necessary. If poll workers are going to presort ballots or take voting machines home with them, we cannot really have much confidence in the audit.

So, in conclusion, if voter-verified paper records are going to be much more than an inconvenience to poll workers and election officials, we really need to use them to check the electronic tally. The debate over voting system security is not really a debate over paper or what technology we use. It is a debate about increasing public confidence in our voting system, and ultimately, good post-election audits are what will increase that public confidence.

[The statement of Mr. Norden follows:]

BRENNAN
CENTER
FOR JUSTICE

Committee on House Administration, Subcommittee on Elections

United States House of Representatives

Statement of

Lawrence D. Norden

Counsel, Brennan Center for Justice at NYU School of Law

March 20, 2007

The Brennan Center for Justice thanks the Subcommittee on Elections for holding this hearing. We appreciate the opportunity to share with you the results of our extensive studies to ensure that our nation's voting systems are more secure and reliable. The Brennan Center for Justice is a nonpartisan think tank and advocacy organization that focuses on democracy and justice. We are deeply involved in the effort to ensure accurate and fair voting, voter registration and campaign finance reform.

I. THE BRENNAN CENTER'S WORK ON VOTING SYSTEM SECURITY AND POST-ELECTION AUDITS

In 2005, in response to growing public concern over the security of new electronic voting systems, the Brennan Center assembled a task force (the "Security Task Force") of the nation's leading technologists, election experts, and security professionals to analyze the security and reliability of the nation's electronic voting machines.[1] One of the key findings of the Security Task Force is by now widely accepted by computer scientists, many election officials, and much of the public: all of the major electronic voting systems in use in the United States have serious security and reliability vulnerabilities.

Many have advocated mandating voter-verified paper records as a solution to these vulnerabilities. In fact, voter-verified paper records by themselves will not address the security and reliability vulnerabilities the Brennan Center and many other groups have identified. To the contrary, as the Brennan Center Security Task Force noted in *The Machinery of Democracy: Protecting Elections in an Electronic World*,[2] voter-verified paper records, by themselves, are "of questionable security value." Paper records will not prevent programming errors, software bugs, or the insertion of corrupt software into voting systems.

---

[1] For a list of the members of the Security Task Force see Appendix A of this Statement.

[2] Lawrence Norden *et al.*, THE MACHINERY OF DEMOCRACY: PROTECTING ELECTIONS IN AN ELECTRONIC WORLD (Brennan Center for Justice ed., 2006) [hereinafter "Brennan Center Security Report"].

Voter-verified paper records will only have real security value if they are regularly used to check electronic tallies. It is for this reason that the Brennan Center urges Congress to adopt meaningful post-election audit legislation as soon as possible. Currently, only thirteen states require both voter-verified records and regular audits of those records.[3]

II. THE GOALS OF AN AUDIT AND HOW TO FULFILL THEM

How to use voter-verified paper records to check or "audit" the electronic records has, until recently, received very little attention, and even less systematic study. In *The Machinery of Democracy*, the Brennan Center made several audit recommendations, based in part on what we viewed as the best practices of the handful of states that already conduct regular audits.

Since the release of that report, the Brennan Center has teamed with the Samuelson Law, Technology & Public Policy Clinic at Boalt Hall School of Law (UC Berkeley), as well as several election officials and leading academics (collectively, the "Audit Group") to evaluate current audit laws and procedures and provide critical analysis to public officials as they begin to adopt audit schemes and procedures.

The Audit Group has identified several questions that legislators should ask before adopting an audit scheme and procedures. Among them are how, whether and to what extent the audits will:

1) increase public confidence in the results of an election;

2) deter fraud against the voting system;

3) detect large-scale, systemic errors;

4) provide feedback that will allow jurisdictions to improve elections and machines in future years;

5) confirm, to a high level of confidence, that a 100% manual recount would not change the outcome of the race.[4]

The Brennan Center has concluded that, among other things, an effective audit scheme that addresses these questions will do the following:

- **Use Transparent and Random Selection Processes for All Auditing Procedures.** Audits are much more likely to prevent fraud, and produce greater

[3] Those states are Alaska, Arizona, California, Colorado, Connecticut, Hawaii, Illinois, Minnesota, New Mexico, New York, Utah and Washington, West Virginia. *See* http://verifiedvoting.org/

[4] This is sometimes described as "confirm that the right candidate was declared the winner," though this is probably more than any statistical audit can guarantee.

voter confidence in the results, if the ballots, machines or precincts to be audited are chosen in a truly random and transparent manner.

- **Allow the Losing Candidate To Select Precinct(s) or Machine(s) To Be Audited.** In addition to conducting random audits, jurisdictions should allow a losing candidate to pick at least one precinct to be audited. This would serve two purposes: first, it would give greater assurance to the losing "side" that the losing candidate actually lost; second, it would make it much more likely that anomalous results suggesting a programming error or miscount were reviewed.

- **Place an Independent Person or Body in Charge of the Audits.** To increase public confidence that the audit can be trusted, it will be helpful to ensure that the person or persons supervising the audit are viewed as independent of the State's chief election officer, vendors who may have sold machines being audited, and any candidate running in an audited race.

- **Implement Effective Procedures for Addressing Evidence of Fraud or Error.** If audits are to have a real deterrent effect, jurisdictions must adopt clear procedures for dealing with audit discrepancies when they are found. Detection of fraud will not prevent attacks from succeeding without an appropriate response. Such procedures should also ensure that outcome-changing errors are not ignored.

- **Encourage Rigorous Chain of Custody Practices.** Audits of voter-verified paper records will serve to deter attacks and identify problems only if states have implemented solid chain of custody and physical security practices that will allow them to make an accurate comparison of paper and electronic records.

- **Audit a Minimum Percentage of Precincts or Machines for Each Election, Including At Least One Machine or Precinct for Each County in the State.** An audit that targets a fixed percentage (*e.g.* 3 percent) of machines or precincts to audit in each Congressional District is an efficient method for catching broad-based error or fraud. By auditing at least one machine or precinct in every county, jurisdictions will greatly increase the likelihood that they will find discrepancies caused by fraud or error at the county level.

- **Record and Publicly Release Numbers of Spoiled Ballots, Cancellations, Over-votes and Under-votes.** Audits that record the number of over-votes, under-votes, blank votes and spoiled ballots (including in the case of DREs, cancellations) could be extremely helpful in uncovering software attacks and software bugs and point to problems in ballot design and instructions.

- **Audit Entire System, Not Just the Machines.** History has shown that incorrect vote totals often result from mistakes when machine totals are aggregated at the tally server. Accordingly, good audit protocols will mandate that the entire system – from early and absentee ballots to aggregation at the tally server – be

audited for accuracy.

- **Increase Scrutiny in Close Elections.** Software bugs and/or tampering that affect the software of a small number of machines will generally not affect the outcome of federal elections. In extremely close races, of course, such problems can change the outcome of a race. In such cases, a 3 percent audit is unlikely to uncover a software bug, programming error or malicious attack that might alter the results of the race. Accordingly, the Brennan Center recommends that exceptionally close races receive heightened scrutiny.

III. BRENNAN CENTER AUDIT RECOMMENDATIONS IN DETAIL

There is a substantial likelihood that the audit procedures and other security countermeasures currently in place in most states would not detect a cleverly designed software attack program. Currently, only twelve of the states that require voter-verified paper records also mandate regular audits of those paper records to ensure that the electronic record is accurate.[5] Moreover, even those states that have mandated regular audits have not developed the best practices and protocols that are necessary to ensure their effectiveness in discovering attacks or failures in the voting systems.

Recommendation #1: Use Transparent and Random Selection Processes.

The development of transparently random selection procedures for all auditing procedures is key to audit effectiveness. This includes the selection of precincts and/or machines to be 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 and, ideally, videotaped.
- The random selection is publicly verifiable, *i.e.*, anyone observing is able to verify that the sample was chosen randomly.
- The process is simple and practical within the context of current election practice so as to avoid imposing unnecessary burden on election officials.

The danger of non-transparent and non-random audits was made plain in Cuyahoga County, Ohio in 2004, when the Libertarian and Green Party Presidential candidates alleged problems with the general election results. In response to these allegations, the state mandated hand counts of ballots cast in 3 percent of the County's

[5] electionline.org, *Case Study: Auditing the Vote* (March 2007), *available at* http://www.electionline.org/Portals/1/Publications/EB17.pdf.

precincts, mandating a full recount if the 3 percent audit revealed discrepancies between the punch-card and electronic records. "Seeking to avoid a vast hand-count of thousands of punch-card ballots, election workers broke state law by pre-sorting the ballots to ensure they matched the final tally."[6] In other words, the audit was rigged to show no problems.[7]

The only way to ensure that we avoid the problems of Cuyahoga County in 2004 is to mandate that the selection of audited precincts be observable to the public and conducted in a truly random manner. The Voter Confidence and Increased Accessibility Act of 2007 (H.R. 811) sets important standards for transparency and randomness by requiring that audits shall be conducted "in a manner that allows for observation by the public,"[8] and that precincts be selected on an "entirely random basis using a uniform distribution in which all precincts" have an equal chance of being selected.[9]

Recommendation #2: Allow Losing Candidate To Select Precinct(s) To Be Audited

Several of the nation's leading experts on election security issues, including Professor Ronald Rivest of MIT, Professor Doug Jones of the University of Iowa and Professor Andrew Appel of Princeton University[10] have advocated allowing a losing candidate to pick additional precincts or machines to be audited. We think some variation of this suggestion is a good idea and endorse the recommendation.

This could be added to a statute as follows:

> At the request of any candidate who appears to have lost under the initial vote count, the chief auditor shall administer additional manual audits of at least [X] precincts or other audited units of the candidate's choosing, provided that the candidate reimburses the State for all expenses related to these requested manual audits, unless State law provides that the candidate need not make such reimbursement.

Such a procedure would serve two purposes: first, it would give greater assurance to the losing candidate and "side" that that the candidate actually lost; second, it would make it much more likely that anomalous results that could suggest a programming error or miscount would be reviewed.

---

[6] *Id.* at 5.
[7] *Id.*
[8] H.R. 811, 110th Cong. § 5 (2007).
[9] *Id.*
[10] *See e.g.* Andrew W. Appel, *Effective Audit Policy for Voter Verified Paper Ballots in New Jersey*, Center for Information Technology and Department of Computer Science, Princeton University (February 22, 2007), *available at* http://www.cs.princeton.edu/~appel/papers/.

Recommendation # 3: Place an Independent Person or Body In Charge of the Audits

Those in charge of the audit are likely to be responsible for selecting precincts or machines, calling for additional audits when anomalies or discrepancies are found, and ensuring that all information from the audit is made public. If the public is to be confident in the effectiveness of the audits, it is critical that these persons are seen as independent of both voting system vendors and candidates running in audited races.

The Count Every Vote Act of 2007 (H.R. 1381) and the Voter Confidence and Increased Accessibility Act accomplish this goal by establishing in each state an independent Chief Auditor and independent Audit Board, respectively.[11]

Recommendation #4: Implement Effective Procedures for Addressing Evidence of Fraud or Error

Audits are of questionable security value, and are far less likely to deter fraud, if jurisdictions do not have effective procedures for action where evidence of machine malfunction and/or fraud is uncovered. In the Brennan Center's extensive review of state election laws and practices, and in its interviews with election officials for *The Machinery of Democracy*, 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 or recount.

The Voter Confidence and Increased Accessibility Act partially addresses these concerns by requiring a full publication of results of the audits, including all discrepancies discovered between the paper and electronic records.[12] We are hopeful that this increased transparency will make state and local election officials more willing to put in place effective procedures for investigating discrepancies when they occur.

We also recommend adding language *that requires* additional audits where discrepancies between the paper and electronic records in the audit are greater than the expected error rates for the relevant voting machines.

Recommendation #5: Encourage Solid Chain of Custody Practices

Audits of voter verified paper records will serve to deter attacks and identify problems only if states have implemented solid chain of custody and physical security practices. Missing or damaged paper or electronic records will make the reconciliation of audits all but impossible.

The Count Every Vote Act takes the important step of requiring the "appropriate State election official" to "develop and implement [...] procedures to monitor and

[11] H.R. 1381, 110th Cong. § 102 (2007); H.R 811, 110th Cong. § 5 (2007).
[12] H.R. 811 at § 5.

document the chain of custody for election ballots, voter verified paper records, software, hardware and vote storage media before, during, and after an election for Federal office."[13]

We endorse this provision and recommend its inclusion in any voting security bill passed by this Congress.

Recommendation #6: Audit a Minimum Percentage of Precincts or Machines for Each Election

An audit that targets a relatively small but fixed percentage (*e.g.* 3 percent) of machines or precincts in each Congressional District is an efficient method for catching broad-based error or fraud. By auditing at least one machine or precinct in every county, jurisdictions will greatly increase the likelihood that they will find discrepancies caused by fraud or error at the county level (*i.e.*, in creating the ballot definition files or programming machines). They will also receive important feedback about the performance of specific machines throughout the state.

In many states, it will be far more efficient to audit by machine or ballot batches, rather than by precinct. Particularly in states that use touch-screen voting machines, jurisdictions will be able to achieve the same level of confidence in their results by auditing a smaller percentage of machines. The Voter Confidence and Increased Accessibility Act gives jurisdictions the flexibility of auditing by machine or vote batches, so long as the National Institute of Standards and Technology approves of their audit mechanism ahead of time.[14]

Recommendation # 7: Record and Publicly Release Numbers of Spoiled Ballots, Cancellations, Over-votes and Under-votes

Audits that record the number of over-votes, under-votes, blank votes and spoiled ballots (including in the case of DREs, cancellations) could be extremely helpful in uncovering software attacks or software bugs. This would be particularly true if such results were made public.

At least one study has purported to show that the majority of voters do not thoroughly check their voter verified paper records.[15] If a voter does not check her paper record, the paper record does not provide extra security for that voter. A vote could be misrecorded on both the paper and electronic record, and the voter (and election officials) would not realize votes were incorrectly recorded.

---

[13] H.R. 1381 at § 101(c).
[14] H.R. 811 at § 5.
[15] Ted Selker and Sharon Cohen, *An Active Approach to Voting Verification* (CalTech/MIT Voting Technology Project, VTP Working Paper #28, 2005) at 2, *available at* http://www.vote.caltech.edu/media/documents/wps/vtp_wp28.pdf.

However, if even a very small percentage of voters check their paper records thoroughly, an unusual number of cancellations on the paper trail will provide evidence that there was some problem in the way the paper record was recording votes.

There is a similar reason for counting over-votes and under-votes on precinct count optical scans. Many voters have benefited from the fact that precinct count optical scan machines have an over- and under-vote protection. If a voter skips a race, or votes for two candidates in a race, the scanner now informs the voter of the error, and allows her to change her ballot, so that her intention will be accurately recorded. In *The Machinery of Democracy,* the Brennan Center demonstrates that a state-wide shut-down of this protection (or a "bug" that accidentally shut it off) could result in the loss of tens of thousands of votes, mostly in low-income communities.[16] A review of the number of over and under-votes in an audit would provide evidence that something went wrong with this protection.

Moreover, this data will be extremely helpful to states, the Election Assistance Commission, academics and election integrity activists in assessing the effectiveness of ballot instruction and layout as well as the performance of specific machines. Post-election audits should be conducted not only to deter fraud and catch errors. They should also be used to provide important information on how well machines, ballots, and voters perform.

The Voter Confidence and Increased Accessibility Act requires the publication of the number of spoiled ballots, cancellations, over-votes and under-votes for each audited precinct or machine.[17]

Recommendation # 8: Audit Entire System, Not Just the Machines

History has shown that incorrect vote totals often result from accidents or tampering when machine totals are aggregated at the polling place or at the county tally server.[18] Accordingly, among other procedures, the Brennan Center has recommended legislative language that will:

- **Ensure That All Polling Places Compare Vote Tallies and Sign-in Sheets.** At close of the polls, vote tallies for each machine should be totaled and compared with number of persons that have signed the poll books. A comparison of these numbers should be made publicly available.

- **Ensure Individual Voting Machine and Precinct Totals Accurately Are Reflected in Tally Server Calculations.** A copy of totals for each machine should be posted at each polling place on Election Night and taken home by poll

[16] Brennan Center Security Report, *supra* note 1.
[17] H.R. 811 at § 5.
[18] *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).

workers to check against what is posted publicly at election headquarters, on the web, in the papers, or elsewhere. This countermeasure allows poll workers 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.

- **Mandate Daily Count of Early and Absentee Ballots.** The same audit procedures should apply to a daily count of early and absentee ballots, including, in the case of absentee ballots, the dates upon which the ballots were mailed and received.

We have not found these requirements in any bills that have been introduced in Congress this year and we strongly urge their inclusion in any voting system security bill that the House considers.

Recommendation #9: Increase Audit Scrutiny in Close Elections

For many races, a 3 percent audit will be more than sufficient to have confidence that a full recount would not result in a different outcome. However, in very close races, such an audit will not provide significant assurance that a software bug, programming error or malicious attack did not alter the results of an election.

This can be seen in the chart below, which looks at a typical Congressional District (the "Model Congressional District") of 400 precincts (for purposes of simplicity, it is assumed that all precincts are of roughly equal size). In this analysis, it is assumed that if more than 20% of the ballots in any single jurisdiction were corrupted, election officials and the public would detect the corruption without an audit (this is a common assumption in academic literature on this subject):

No. of Precincts in Congressional District	Margin of Victory	Confidence Level Attained By 3% Audit[19]
400	5%	80%
400	1.75%	43%
400	0.75%	22%

As the chart above shows, as the race gets closer, we have less confidence that the 3 percent audit will catch a corruption of the electronic record that could have altered the results of an election. The reason for this is simple: if a race is decided by a margin of greater than 5 percent, a software bug that actually changes the result of the election will probably have to affect a fairly large number of votes. A 3 percent audit has a relatively good chance of catching such a wide-spread error. By contrast, the outcome of an election that is decided by only 1 percent of the votes could be affected by a software bug that corrupts only a small number of votes. It is unlikely we will find these corrupted or misprogrammed machines if we audit only 3 percent of a district's precincts.

[19] In districts with less than 400 precincts, or with wide variation in number of votes per precinct, these confidence levels will be even lower.

If we increase the percentage of precincts or machines to be audited in close races, we can at least partially address this problem. The Voter Confidence and Increased Accessibility Act attempts to do this by adopting a "tiered" adjustable audit. The boxed numbers represent the confidence level achieved in the Model Congressional District by this bill's proposal.

No. of Precincts	Margin of Victory	Probability in a 2% Audit	Probability in a 3% Audit	Probability in a 5% Audit	Probability in a 10% Audit
400	0.75%	15%	22%	34%	57%
400	1.75%	31%	43%	61%	86%
400	5.00%	66%	80%	94%	99%

Under this "tiered" approach, jurisdictions will have greater confidence that result-changing errors were caught than they would get from a flat, 3 percent audit for all races.[20]

The approach adopted in the Voter Confidence and Increased Accessibility Act seeks to balance the need to increase scrutiny in close elections with the legitimate concern of election officials that they should not be overburdened by uncertain and administratively costly audits. This can be seen in the chart below, which shows the number of federal races in recent history with margins that would have triggered the tiered audits set forth in the Act. In short, the number is exceedingly small – in a typical federal general election, the vast majority of states would not be required to conduct even a single increased audit.

Year	Federal Races Requiring 3% Audit (decided by more than 2% margin)	Federal Races Requiring 5% Audit (decided by between 1% and 2% margin)	Federal Races Requiring 10% Audit (decided by between 0% and 1%)
2002	461	3	4
2004	510	5	5
2006	451	7	10

In 2002, 2004, and 2006, having a tiered audit procedure as proposed in the Voter Confidence and Increased Accessibility Act would have had a cost that was negligibly greater than a flat audit of 3 percent, since almost all of the races would have been audited at the 3 percent level anyway (the first tier). The extra cost of performing some audits in the second and third tier contributes about 1/30th of the total audit cost.[21]

---

[20] As some commentators have noted, where Congressional Districts have less than 400 precincts, or precincts that vary substantially in size, the confidence levels listed in this chart will fall. Nevertheless, the basic concept remains the same: by increasing the audit percentage in close races, we gain greater confidence that result-changing errors will be caught. *See e.g* Ronald Rivest, *On Auditing Elections When Precincts Have Different Sizes*, Computer Science and Artificial Intelligence Laboratory, Massachusetts Institute of Technology (March 18, 2007), *available at* http://theory.csail.mit.edu/~rivest/Rivest-OnAuditingElectionsWhenPrecinctsHave-DifferentSizes.pdf, and Howard Stanislevic, *Random Auditing of E-Voting Systems. How Much is Enough*, *available at* http://www.votetrustusa.org/pdfs/VTTF/EVEPAuditing.pdf.

[21] This calculation assumes that costs of increased audits increased linearly with audit percentage.

Although having a tiered approach adds some complexity to the process, it does not add significantly to the cost of doing the audits; yet it increases one's confidence that election results are correctly reported for all races—even close races.

Moreover, there is already significant precedent in state law for the percentages established by these tiers. Several states already require and successfully complete post-election audits of 3, 5 and 10 percent of precincts or machines.[22] It should be noted that *some of these audits include dozens of races and ballot questions, as opposed to the one, two or (at most) three federal races that each Congressional District will be mandated to audit under the Voter Confidence and Increased Accessibility Act.*

Finally, and importantly, the Voter Confidence and Increased Accessibility Act leaves room for states to develop their own audit schemes, so long as the schemes provide an equivalent minimum level of confidence as the tiered, precinct based approach. This is significant for two reasons. First, it should allow jurisdictions to audit by machine, ballot batches, or other audit units. In many cases, this will greatly reduce the administrative cost and burden of the audit requirements. For instance, in states where there are more voting machines than precincts, auditing by machine should allow jurisdictions to audit fewer total ballots.[23] Second, it gives jurisdictions great discretion to study and develop innovative auditing mechanisms that may be specifically appropriate for their states.

The Brennan Center recommends slight modifications to the alternate audit mechanism in the Voter Confidence and Increased Accessibility Act to ensure that these goals are met, and to provide states with guidance from the National Institute of Standards and Technology as they develop alternative audit mechanisms. Specifically, we would change the language to read as follows:

> Use of Alternate Mechanism – Notwithstanding subsection (a), a State may adopt and apply an alternative mechanism to determine the number of voter-verified paper ballots that will be subject to the hand counts required under this subtitle with respect to an election for Federal office, so long as the National Institute of Standards and Technology determines that the alternative mechanism is as transparent as the procedure under subsection (a) and is consistent with the guidelines set forth in Section X.

---

[22] For instance, of the twelve states that require voter-verified paper records and post-election audits, Hawaii mandates the post-election audits of 10 percent of all precincts, Illinois mandates audits of 5 percent of all precincts, Colorado and West Virginia mandate audits of 5 percent of machines, Alaska mandates audits of enough precincts to account for at least 5 percent of all votes, and New York mandates audits of 3percent of all machines. Connecticut's Secretary of State recently introduced legislation that would require a post-election audit of 20 percent of its precincts. electiononline.org *supra* note 3, at 12-17.

[23] The confidence level in any audit fundamentally depends on the number of units audited; the greater the number of audit units (precincts, machines, etc.), the greater the confidence. If a jurisdiction can audit the same number of units with fewer ballots per unit, it will maintain statistical confidence in its audits while reducing its administrative burden.

Section X -- GUIDANCE ON BEST PRACTICES FOR ALTERNATIVE AUDIT MECHANISM. Not later than May 1, 2008, the National Institute for Standards and Technology shall establish guidance for States to establish alternative audit mechanisms. Such guidance shall be based upon scientifically reasonable assumptions for the purpose of creating an alternative audit mechanism that will

"(a) require the hand-count of at least 2% of all precincts (or other audited units) within each Congressional District, and ensure, with at least [90/95/99]% statistical confidence, for each federal election held in the State, that a 100% manual recount would not alter the outcome of the election; or

"(b) be at least as effective as section 322(a) in ensuring that for each federal election held in the state, a 100% manual recount would not alter the outcome of the election.

AUTHORIZATION OF APPROPRIATIONS – There are authorized to be appropriated to the National Institute of Standards and Technology $100,000 to establish the guidance required by this section.

In conclusion, many of the nation's leading election and security experts have reviewed the tiered audit scheme adopted by the Voter Confidence and Increased Accessibility Act and have concluded that it is a clear improvement over a flat percentage audit for all races. They have stated that it "reasonably balances a number of interests: confidence in election results, deterrence of electoral fraud, audit cost, innovation in new audit designs, and the burdens of administrability and frequency of increased percentage audits." A copy of their analysis is annexed to this statement as Appendix B.

IV. CONCLUSION

The nation's move to electronic voting has had many benefits, including increased accessibility for disabled voters and increased efficiency in election administration. Unfortunately, academic studies and Election Day problems over the last several years have shown that these new machines also came with a cost: new security and reliability problems, as well as increased public doubt about the accuracy and fairness of our elections.

This does not mean that the move toward electronic voting was a mistake. The mistake would be to fail to develop federal standards and procedures for these new machines. Most importantly, if we are serious about addressing the unique security and reliability vulnerabilities of these new machines, Congress must adopt solid post-election audit legislation as soon as possible.

APPENDIX A: 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

APPENDIX B: MEMO ON H.R. 811 AUDIT MECHANISM

To: Congressman Rush Holt

From:* Lawrence Norden, Brennan Center for Justice at NYU School of Law

Aaron Burstein, Samuelson Law, Technology & Public Policy Clinic, UC Berkeley School of Law

Joseph Hall, School of Information, UC Berkeley

David L. Dill, Department of Computer Science, Stanford University

Candice Hoke, Director, Center for Election Integrity, Cleveland State University

Walter Mebane, Department of Government, Cornell University

Freddie Oakley, Yolo County, CA, Clerk-Recorder

Ronald L. Rivest, MIT EECS Department

David Wagner, Department of Electrical Engineering and Computer Sciences, UC Berkeley

Date:** 1 February 2007

Re: Thoughts on Mandatory Audits

We write to support your decision to adopt a "tiered" approach to auditing of voter verified paper records in the Voter Confidence and Increased Accessibility Act of 2007. Our understanding is that the language in the bill is as set forth in Appendix A.

This replaces earlier language that would have required all states to audit 2% of all precincts under all circumstances. We believe the new language will give jurisdictions more confidence that they will catch programming errors, software bugs or attacks against voting systems. This audit scheme also seems to allow jurisdictions to develop other, innovative audit procedures on their own and still receive federal funding for such audits, as long as they are at least as effective as what is otherwise required. Finally, this scheme minimizes potential burdens on election officials by requiring increased levels of audits *only when races are exceptionally close.* Below we explain the reasons behind our consensus.

---

* The authors' affiliations are provided for identification purposes only. The views expressed in this memorandum are the authors' personal views. The authors do not purport to represent the views of their respective institutions.

** Updated on March 19, 2007

Discovery of Systemic Error vs. Confidence Level and the Development of the Tiered Auditing Approach

Some of your colleagues may want to know what percentage of precincts must be audited in order to ensure that there is not an "unacceptable" level of error.

In truth, it may be that attempting to prevent an "unacceptable" level of error on electronic voting machines through audits is too administratively burdensome. This is particularly true if we assume that a certain number of votes (e.g., 10 % or 20%) can be miscounted in a single polling place without giving rise to an independent investigation, and that some errors will be "clumped" into a relatively small number of precincts, rather than spread evenly among them.

Thus, we might say that the miscounting of 1% of all votes in a federal race is "unacceptable." In an imagined typical congressional district, with 400 precincts of roughly equal size, we would need to audit more than 10% of all precincts to have at least 90% confidence that an audit would discover an error causing a miscounting of 1% or more of the votes.

Mandating a 10% audit for all races would be a high burden on many States. And in the vast majority of races, a shift of 1% of the votes would not alter the outcome of the race. For that reason, we might say that while less than ideal, we are willing to live with the risk that audits will not catch the 1% counting error in races where such an error is not going to change the outcome of the race.

But in races decided by less than 1% (in recent history, this has represented less than one percent of all federal elections), we might say we are *unwilling* to accept this risk.

Typical Congressional District

It is therefore worth considering how well the tiered approach will perform if we ask how likely audits in this scheme are to detect errors that would change the outcome of a specific race. The table below gives the probabilities of detecting discrepancies in 2, 3, 5 and 10% post-election audits in a typical congressional district with 400 precincts for races with margins ranging from 0.5% to 5.0% (Note: the highlighted numbers give confidence levels for audits conforming to the tiered approach of the Voter Confidence and Increased Accessibility Act of 2007.)[24]

No. of precincts	Margin of victory	Probability in a 2% audit	Probability in a 3% audit	Probability in a 5% audit	Probability in a 10% audit
400	0.50%	10%	14%	22%	41%
400	0.75%	15%	22%	34%	57%
400	1.00%	18%	27%	40%	66%
400	1.75%	31%	43%	61%	86%
400	2.00%	33%	46%	65%	89%
400	5.00%	66%	80%	94%	99.6%

[24] These calculations assume that a vote shift of 20% or more within a single precinct will be detected.

As you can see from this chart, in cases of narrow margins, adopting the tiered approach could give the public and jurisdictions considerably greater confidence that result-changing errors were caught than would a fixed-percentage audit, without putting an unreasonable burden on the vast majority of districts. [25]

Minimizing the Burden on Election Officials

This tiered audit approach has the benefit of providing increased security in close elections without placing an undue burden on election officials. We can see this in the chart below, which shows the number of Congressional races in recent history with margins that would have triggered the tiered audits set forth in the Act. If your audit scheme were required in the last three federal elections, the number of expanded audits would have been exceedingly small.

Year	Federal Races Requiring 3% Audit (decided by more than 2% margin)	Federal Races Requiring 5% audit (decided by between 1% and 2% margin)	Federal Races Requiring 10% audit (decided by between 0% and 1%).
2002	461	3	4
2004	510	5	5
2006	451	7	10

Thus, we see that in 2002, 2004, and 2006, having a tiered audit procedure as proposed in the Holt bill would have a cost that is negligibly increased compared to a flat audit of 3%, since almost all of the races would be audited at the 3% level anyway (the first tier). The extra cost of performing some audits in the second and third tier contributes about 1/30th of the total audit cost.[26] Although having a tiered approach adds some complexity to the process, it does not add significantly to the cost of doing the audits; yet it greatly increases one's confidence that election results are correctly reported for all races—even close races.

The tiered audit scheme adopted by the Holt Bill reasonably balances a number of interests: confidence in election results, deterrence of electoral fraud, audit cost, innovation in new audit designs, and the burdens of administrability and frequency of increased percentage audits.

---

[25] As some commentators have noted, where Congressional Districts have less than 400 precincts, or precincts that vary substantially in size, the confidence levels listed in this chart will fall. Nevertheless, the basic concept remains the same: by increasing the audit percentage in close races, we gain greater confidence that result-changing errors will be caught. *See e.g.* Ronald Rivest, *On Auditing Elections When Precincts Have Different Sizes,* Computer Science and Artificial Intelligence Laboratory, Massachusetts Institute of Technology (March 18, 2007), *available at* http://theory.csail.mit.edu/~rivest/Rivest-OnAuditingElectionsWhenPrecinctsHave-DifferentSizes.pdf, and Howard Stanislevic, *Random Auditing of E-Voting Systems. How Much is Enough*, *available at* http://www.votetrustusa.org/pdfs/VTTF/EVEPAuditing.pdf.

[26] This calculation assumes that costs of increased audits increased linearly with audit percentage.

Appendix A

The text of the tiered audit used by the Voter Confidence and Increased Accessibility Act of 2007:

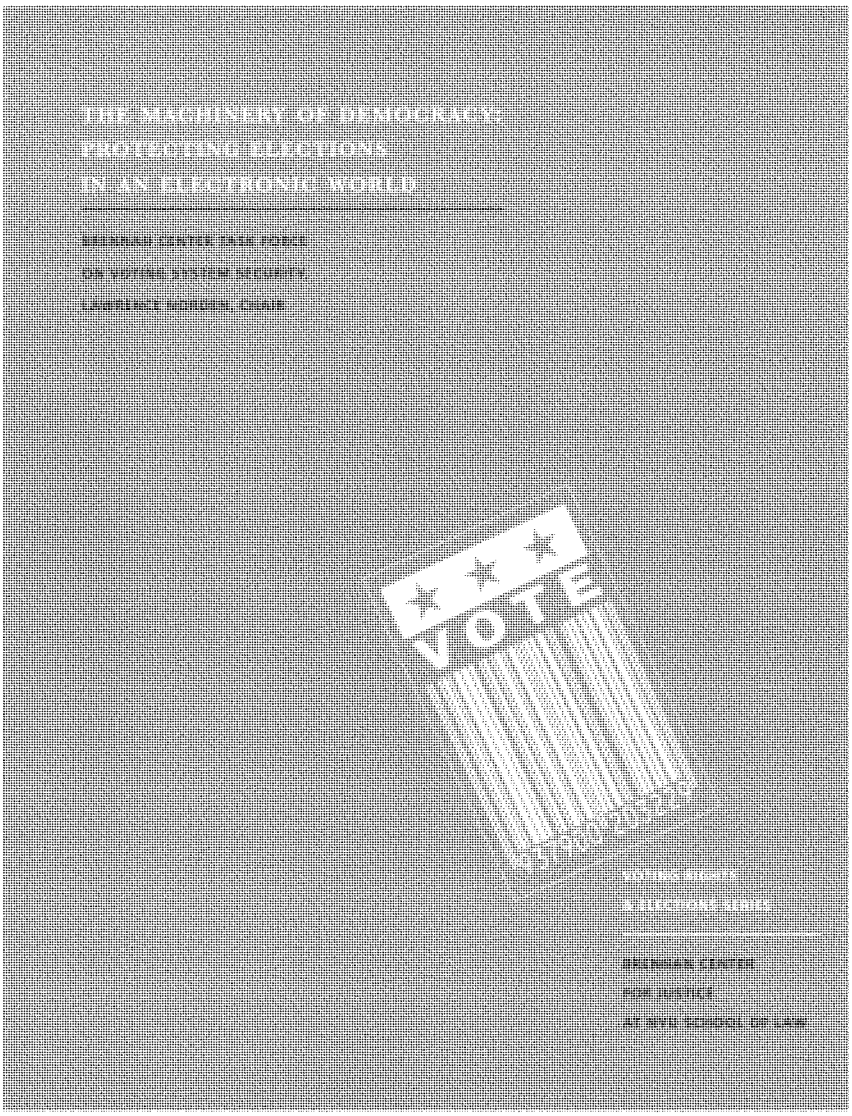
(a) IN GENERAL.—Except as provided in subsection (b), the number of voter-verified paper ballots which will be subject to a hand count administered by the Election Audit Board of a State under this subtitle with respect to an election shall be determined as follows:

(1) In the event that the unofficial count as described in section 323(a)(1) reveals that the margin of victory between the two candidates receiving the largest number of votes in the election is less than 1 percent of the total votes cast in that election, the hand counts of the voter-verified paper ballots shall occur in 10% of all precincts (or equivalent locations) in the Congressional district involved (in the case of an election for the House of Representatives) or the State (in the case of any other election for Federal office).

(2) In the event that the unofficial count as described in section 323(a)(1) reveals that the margin of victory between the two candidates receiving the largest number of votes in the election is greater than or equal to 1 percent but less than 2 percent of the total votes cast in that election, the hand counts of the voter-verified paper ballots shall occur in 5% of all precincts (or equivalent locations) in the Congressional district involved (in the case of an election for the House of Representatives) or the State (in the case of any other election for Federal office).

(3) In the event that the unofficial count as described in section 323(a)(1) reveals that the margin of victory between the two candidates receiving the largest number of votes in the election is equal to or greater than 2 percent of the total votes cast in that election, the hand counts of the voter-verified paper ballots shall occur in 3% of all precincts (or equivalent locations) in the Congressional district involved (in the case of an election for the House of Representatives) or the State (in the case of any other election for Federal office).

(b) USE OF ALTERNATIVE MECHANISM.—Notwithstanding subsection (a), a State may adopt and apply an alternative mechanism to determine the number of voter verified paper ballots which will be subject to the hand counts required under this subtitle with respect to an election, so long as the National Institute of Standards and Technology determines that the alternative mechanism will be at least as effective in ensuring the accuracy of the election results and as transparent as the procedure under subsection (a).


THE MACHINERY OF DEMOCRACY:
PROTECTING ELECTIONS
IN AN ELECTRONIC WORLD
BRENNAN CENTER TASK FORCE
ON VOTING SYSTEM SECURITY
LAWRENCE NORDEN, CHAIR
VOTE
VOTING MODE
TECHNOLOGY
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

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

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.

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.

■ 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 further 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.*

6

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.

8

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 bave 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.[59]

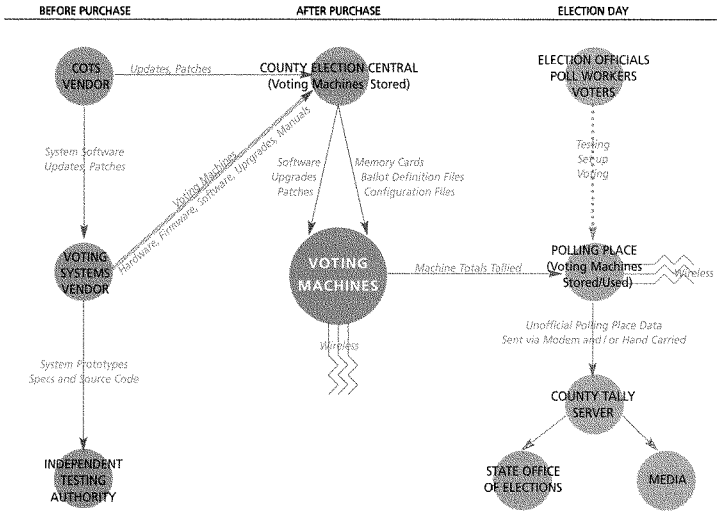
■ NINE CATEGORIES OF ATTACKS

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 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.

The least difficult attacks are centralized attacks that occur against the entire voting system.

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

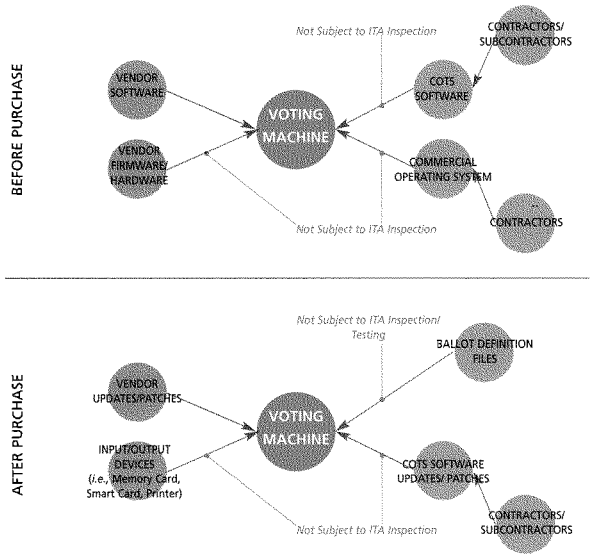
The process for developing voting system software is not dramatically different from the development of any other type of software or operating systems. Vendors develop a set of requirements for their machines; a team of programmers is subsequently assembled to apply those requirements by developing 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.

46

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 beuefit (*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

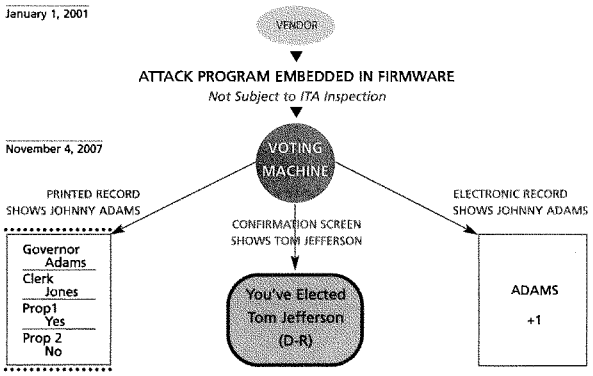
- Number of DREs w/VVPT in 3 largest counties: 9,634[149]

- 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.[156] 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 hy 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 ont 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. 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.

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.

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 uncorrectly 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 Batdeground 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/papertrailboycot.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/emkiqfxphochfss2s5anfuxbgj3zgpkv557moi3vb6f3ne44mcni2thdvoywyjcigyeoykwru53mopaa6kt2uxh7ofe/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)	Numbes 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

$$\text{Probability[detect attack]} = 1 - (1 - C)^N$$

Writing the probabilities as percentages, this looks like:

$$\text{Probability[detect attack]} = 100\% - (100\% - C)^N$$

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 $(1 - C)^8$ 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 shnw 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;

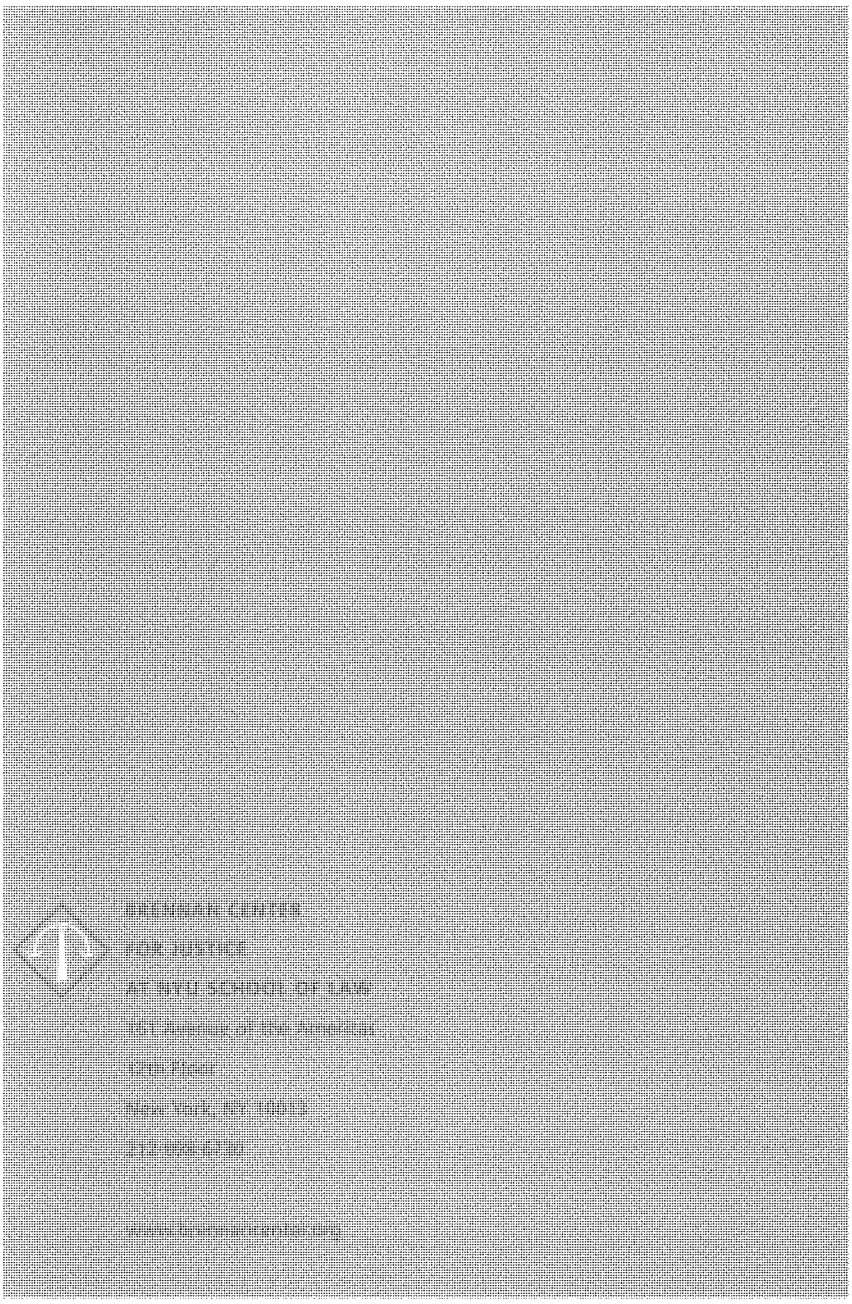
4. Based upon the (a) margin of victory, (b) number of machines affected, and (c) nature and scope of the tampering, determine whether there is a substantial likelihood that tampering changed the outcome of a particular race; and

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

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

Ms. LOFGREN. Thank you very much, Mr. Norden.
Ms. Patrick.

STATEMENT OF TAMMY PATRICK

Ms. PATRICK. Madam Chair, members of the committee, thank you.

My name is Tammy Patrick. I am the Federal Compliance Officer for the Elections Department in Maricopa County, Arizona. In last November's general election, we conducted a statutory hand-audit of 2 percent of the precinct-cast ballots and 1 percent of our early ballots in a total of four races that combined both Federal and State offices. I refer you to my written testimony for more information on that audit, and I am going to confine my oral remarks to three very brief points.

First of all, a little background. Maricopa County has 1.5 million registered voters, 1,142 voting precincts, and about half of our voters vote by mail-in early ballots. At the same time that we were conducting this new hand-audit, we also had well over 100 workers working from 6:00 in the morning to 12:00 p.m. Midnight, processing our provisional ballots. We had difficulty securing the 144 individuals who were needed to conduct the hand recount of that 1 percent of the early ballots and 2 percent of the ballots cast at the precinct. We also had additional difficulty keeping them long enough to actually finish the audit. I cannot fathom how we would conduct a hand-audit of 10 percent of the ballots, especially under the requirements of H.R. 811.

Secondly, it is critical to recognize the limits of a human count. For example, our procedures manual, which is written by the Secretary of State, directed audit boards to count ballots in lots of 25. We found that, in application, that was too difficult. It seems easy enough, but in fact, we had several boards that we had to instruct to stack in groups of 10 in order to have the counts come out correctly. Our State law did not expect perfection from the human count and recognized an acceptable variation between the hand-audit and what was done by the machine tabulation. We could not identify and address every discrepancy as required by H.R. 811 within any realistic time frame. An example of this would be in instances where, in one precinct, the audit board and the electronic machine came up with the exact same number of ballots but had discrepancy in the total number of votes cast, so the boards were not quite understanding in some instances an overvote, for instance, they voted for two when it should have only been for one, so they allocated each one of those to two separate candidates.

Finally, it goes without saying that we cannot conduct a recount that includes provisional ballots until we have finished counting them. The requirements in H.R. 811 to retain the paper ballots, including those cast on a DRE, in a manner so as not to enable them to be tied to a voter, would either preclude any provisional ballot from being cast on a DRE or it would immediately impact the ability of the audit's totals to match reported totals. So, by virtue of the parameters set forth in H.R. 811, a successful hand-audit is impossible. Additionally, we could not sort early ballots in with our election day ballots, as required by H.R. 811 without compromising the inherent security of random order retention. Although we re-

port our results of our early ballots at a precinct level, we tabulate and store them in a random, mixed batch as they come in from the post office, and that is how we count to preserve both the security and the privacy of the voter. So, in our audit, we take those batches of 200 and audit them in their entirety as a batch, and we would not be able to do that, thus resulting in those ballots being handled multiple times.

We are very fortunate that everyone in this room has a common purpose. Whether you are an election official responsible for conducting and tabulating an election, a political observer overseeing this process, an elected official whose name appears on the ballot or all of us simply as voters ourselves, the outcome of the election is that we are all working for the same end, that it is an accurate reflection of the will and intent of the people. But the ability to administer an audit and to implement change in response to the unique environments within which we all work on our local jurisdictional level is an integral characteristic of success of such an audit and must remain at the local level.

I thank you for the opportunity to testify today, and I look forward to answering any questions.

[The statement of Ms. Patrick follows:]

Maricopa County Arizona
Helen Purcell, County Recorder
Karen Osborne, Elections Director

March 20, 2007

Madam Chairman and members of the Committee on House Administration:

We are fortunate that today we are all have a common purpose. Whether you are an Election Official responsible for conducting and tabulating an election, a political observer overseeing the process, an elected official whose name appears on the ballot, or all of us as voters ourselves, we all are working for the same end: that the outcome of the election is an accurate reflection of the will and intent of the people. A hand audit, by definition, is conducted to ensure that the tabulation equipment being used is correctly calculating the vote cast.

Maricopa County has 1.5 million registered voters, 1142 voting precincts, and half our voters vote by mail-in early ballots. At the polling place we have optical scan equipment which the vast majority of our voters utilize. We supplement that system with touch screen voting machines with printers for individuals who need them in order to vote independently, this equated to less than 300 votes out of the almost half million cast at the polls in last November's General Election.

That election saw the implementation of a statutory hand audit requirement of 2% of the precinct-cast ballots and 1% of early ballots. In Maricopa County that translated into 24 precincts, 6 precincts from each of the 4 selected races, and 4,800 early ballots. Both the physical paper ballots as well as the paper record of the votes cast on the touch screens are included; but Provisional ballots, Conditional Provisional Ballots (those awaiting the voter to return with ID), and Write-In Ballots are not. The political parties are required to each provide 72 individuals to conduct the audit thus providing them another involvement opportunity in the oversight of the process.

In the 10 days following a General Election Maricopa County has well over 100 workers processing Provisional Ballots. Working from 6 am to 12 midnight we are able to ensure that a voter who has cast their ballot provisionally in their new home precinct or with a new, married name has their registration updated and their vote processed rather than discredited due to a lack of their updating of registration information; provisional ballots in the traditional sense are less than 1% of what are labeled "provisional" in Arizona. At the same time we were orchestrating the 144 individuals from the public who were participating in the hand audit.

The audit had many challenges. There were only 5 precincts which had ballots cast by voters on the touch screen machines. Statute requires that the process follow the Secretary of State's Procedures Manual which directs the audit boards to count the ballots in lots of 25. Although that seems reasonable, in application many of the boards had to be re-directed to count in 10s due to human errors in counting. If a count did not match a second count was done with a stacking method. The expansion of the audit is only done if the variance is greater than the difference between votes count, divided by the electronic count. We did not encounter any audited precincts which exceeded this variance. This acknowledgement of the human condition is imperative in maintaining the intended purpose of machine tabulation oversight.

The inclusion of Provisional Ballots, which by virtue of this same proposed legislation are not able to be preserved in a manner that makes them possible to be associated with a voter and thus have their tabulation status noted—designating a provisional ballot that was counted versus one that was not— would easily account for variation in totals. Additionally, the specificity outlined on which Early Ballots are to be audited would create dramatic ramifications on the local level. In Maricopa County we process and tabulate Early Ballots in the random mixed batches as they are returned yet the results are reported back to the precinct level. The physical ballots remain in their mixed batches. To sort them would mean handling the ballots numerous additional times and diminish the inherent security that the random order retention affords.

After only one hand audit the state legislature has already seen amendment language to address some of these challenges. Some of the issues can be resolved with simple modification of the Procedures Manual, while others will require legislative changes. The ability to administer the audit in a manner that will function on the local jurisdictional level, and to implement swift changes in response to the unique environments within which we all live, is an integral characteristic of the success of such an exercise.

Respectfully submitted,

Tammy Patrick
Federal Compliance Officer
Maricopa County Elections Department
Maricopa County Arizona

tpatrick@risc.maricopa.gov
602.506.1270

Ms. LOFGREN. Thank you very much.
Our final witness is Ms. Pamela Smith.

STATEMENT OF PAMELA SMITH

Ms. SMITH. Thank you, Chairman Lofgren and Ranking Member McCarthy and members of the committee. Thanks for the opportunity to be here and to testify today.

VerifiedVoting.org and the Verified Voting Foundation were actually started by a computer scientist. We believe that, if our voting systems are reliable and those election officials and the voting public have a way to assure themselves that they are accurate, then that will go a long way to increasing public confidence and, therefore, participation in the process.

We think transparency in elections is so important that we launched an election transparency project in 2006 to promote observation of all phases of the election by citizens, including the audits. We think a key purpose of an election audit is to convince the losers that they have lost. The winners pretty much always think they have won, so that part is easy. I will confine my remarks today to talking a little bit about the successes that States have seen that are doing audits already and also about costs.

Not every State has voter-verified paper records that they can audit at this time, but of those that do, still only a fraction are doing statewide audits. In the ones that are doing statewide audits, there have been successes that illustrate that audits can be done effectively and cost-effectively, and Congress can help us make our elections more transparent and reliable by passing a requirement.

A great example of what an audit can tell us about a voting system, not just about the accuracy of the outcome but about the system itself, occurred in a place that does not yet require audits. Pottawamie County, Iowa, in June of 2006, on the election night of the Republican primary, an experienced county election official there by the name of Marilyn Jo Drake noticed something odd in the vote tallies when the returns were coming in. A popular incumbent seemed to suddenly be losing to an unknown newcomer who had scarcely even campaigned. On her own authority, she performed an audit of a single sample precinct to see if the voting machines were counting correctly. They were not. There was a programming error, which meant that votes for candidate A started going to candidate B. A full hand-count showed the correct result. The machine count was wrong. Suppose both candidates had been unknown, neither one an incumbent, nothing to give her the idea that something was amiss. A routine audit would still have uncovered the problem. Ms. Drake could have just chosen expediency over accuracy. There was no rule requiring her to do this audit. It made more work, but it resulted in two important things—the right candidate's being seated in office and the exposure of a glitch in the system that could then be repaired or prevented the next time.

Auditing really means choosing accuracy over expediency. Yes, it takes some time. Yes, there is some cost involved, but if it is going to be a safety net for voter intent, we have to see it as just one step in what it takes to get our elections right. It is no different than taking care to program the right names on the ballot or recruiting enough poll workers for election day, and you cannot just

do it once in a while. You have to do audits every time. You cannot say, "See, the tallies match every time. Now we do not have to do this anymore." that would be a dangerous perspective that fails not only to comprehend voting system security but also Murphy's Law. There will be problems at every election. What audits and voter-verified paper records do is make those problems solvable.

To talk about costs just a little bit in the States, there is workload. There is a big difference in what one State is doing compared to another, but interestingly, some of the States are actually increasing the amounts that they audit, voluntarily choosing to expand their law or go higher.

What does this add to the budget? It is far from prohibitive. In some cases, the cost is very low, indeed. One of your key costs is what you pay the people doing the counting, plus your supervisory and planning costs, of course. It takes a time—a big difference in time is as variable as the type of ballots you audit. Paper ballots are much easier to count than thermal paper rolls.

What would this look like as a national investment? From what we have been able to find out from the States, it just would not cost that much, but to compare, take the Washington State gubernatorial recount from 2004. The actual cost total was about $900,000. They looked at one race on 2.8 million ballots. It worked out to about 31 cents a ballot. If the provisions in H.R. 811 had been in effect in 2004, nationwide, we would have audited just under 7,000 precincts, and nationwide, we would have checked votes from two or three races per ballot, call it 11.5 million votes checked. Even at a more conservative rate of, say, 35 cents a ballot, it is a little over $4 million. It is not that much.

What we recommend is for audits to be effective, ensure the selection process is verifiably random; make sure the audit happens after all of the ballots have been counted and initial results are in; include all of the ballot types, including absentees. You know, I wanted to say that, as to absentee ballots, it is important to be able to track those for also being able to secure the vote and to secure the chain of custody, so whatever we could do to track absentees is important. Make sure that officials invite the public in to observe. Do not just allow them in, but actually invite their participation, and they will appreciate that and participate more as time goes forward.

Thank you so much.

[The statement of Ms. Smith follows:]

Written Testimony of
Pamela Smith, President, VerifiedVoting.org
Before the Committee on House Administration,
Subcommittee on Elections
U.S. House of Representatives
March 20, 2007

Chairwoman Lofgren, Ranking Member McCarthy, committee members, thank you for the opportunity to testify today. My name is Pamela Smith. I am President of VerifiedVoting.org and the Verified Voting Foundation, partner organizations that promote reliable and publicly verifiable elections. We believe ensuring that our election systems are reliable and publicly verifiable enfranchises voters and increases public confidence and participation in our political process.

My interest in voting issues includes experience as an election observer, locally and internationally. I have testified on verified voting issues in several states, co-authored written testimony on several state voting system Requests for Proposals and legislative recommendations, as well as reports on audit provisions, escrow provisions, election transparency, and accessibility and auditability issues for voting systems.

The focus of my testimony today is Election Audits, a key purpose of which is to convince the losers and their supporters that they've lost. (The winners always believe that they've won.) Audits are one of the most important means for ensuring the accuracy of election outcomes, and for allowing observers to verify that accuracy. There is a strong consensus among those who study election security about what is needed to make audits effective, but implementation has lagged.

Voter-verified paper ballots are essential to ensure that elections can be audited. Nationally, some three quarters of the states now have voter-verified paper records of some kind to audit, but only one quarter have audit requirements, and those are not carried out at all uniformly. Still, successes in some states show that audits can be done effectively and at relatively low cost. Congress can help make our elections more transparent and reliable by passing a federal requirement for voter-verified paper ballots and mandatory random manual audits.

I. Overview of Election Audits

Voting systems are supposed to record and tally the votes that express the will of the voters in electoral contests. Given that no system is perfect, in order to ensure that the will of the voters is *accurately* captured by the voting system and the outcomes are correct, election officials must deploy safety-checks on the entire system. Contest-specific recounts sometimes will clarify the outcome in particularly close races, but the bar to initiating full recounts is high so they are too intermittently applied to serve as an essential spot-check. Instead, officials must conduct random manual audits of a smaller set of ballots.

A random manual audit means that ballots to be audited are selected through a random process and counted manually, and the resulting hand tallies are compared with tallies made by the voting system to check for accuracy. In cases where the tallies differ, additional records may be audited to determine the outcome.[1] Even where an outcome is not changed, discrepancies can provide information about how the system is working. (For this reason, discrepancies should be examined and explained even if they leave an outcome unchanged.)

Election audits must examine enough records, and must do so in a rigorous way. An audit is not effective unless sufficient records are selected,[2] the selection process is truly random, the timing of the audit occurs after the initial tallies have been made public, the types of ballots to be audited include all types, and the record to be audited is a hard copy representation of voter intent – in other words, the voter had the opportunity to confirm that the record accurately represented his or her intent, e.g. a voter-verified paper ballot.[3] And that paper ballot is counted manually—as one state's law puts it, "hand to eye".[4]

Another crucial component of an effective audit: the whole process must be publicly observable. Transparent processes increase the public's confidence in the outcome. Citizen observers should be notified about and invited to watch both the selection process and the actual hand counting of the paper records.

Finally, before the audit begins, procedures should be defined governing what to do if the tallies do not match. Since the voter verified paper ballots are verified by the voter and electronic records are not, the manual tally of the voter-verified paper ballots must be considered the correct record of the vote, except where convincing evidence shows the paper record of voter intent was compromised to the point of being unusable or illegible. If discrepancies occur, an expanded audit and investigation may be needed to clarify the outcome.

If we are not careful, auditing can degrade into meaningless ritual. If the audit is to be a **safety net for voter intent**, those responsible must see this process as one key step in what it takes to get elections right, no different than taking care to program the right names on the ballot every time, or to recruit enough pollworkers for Election Day.

---

[1] Other checks and balances to help ensure accuracy of vote counts include ballot accounting procedures which can and should be carried out for each election, e.g. checking the number of voters who signed in against the number of ballots cast, but the focus of this testimony is on post-election audits carried out after the initial canvass and before the election results are certified.

[2] Significant discussion by a number of experts on what constitutes a sufficient quantity or percentage to audit is ongoing. Better ideas are still emerging. For this reason, proposed legislation such as HR811, the Voter Confidence and Increased Accessibility Act and HR1381, the Count Every Vote Act, appropriately establish not only one tiered scheme for audits but also a provision for alternative auditing schemes, provided those schemes are demonstrated to be at least as effective as the tiered scheme.

[3] The Help America Vote Act (HAVA) seemed to provide for auditable paper records, but it failed to connect the crucial dots between a voter's verification of the paper ballot, and the use of that voter-verified paper ballot in any audit. Proposed amendments to HAVA such as HR811 can remedy that problem.

[4] North Carolina, http://www.ncleg.net/Sessions/2005/Bills/House/HTML/H1024v7.html

Many officials grasp the concept of doing audits, and doing them right – using the voter-verified paper records for the audit, for example, instead of a meaningless end-of-day printout voters have never seen. Some officials, however, may claim that two or three sets of matching tallies prove the system is accurate. They may conclude incorrectly that there's no need to do audits every time. That's like saying that a corporation was audited once and everything was in order, so it's not necessary to audit them again. It is a dangerous way to think about auditing any system.

Such a perspective fails to comprehend the nature of voting system security—and ignores Murphy's Law as well. **Audits really are part of the solution,** not the problem. Problems *will* occur in every election; properly conducted audits using voter-verified paper ballots enable most such problems to be resolved.

II. State Audit Requirements

While many states now have voter-verified paper records to audit, only about one-quarter of the states actually require audits. There is much to be learned from the experiences of those few. Some states have proved that auditing can work, but a federal requirement is needed.

A federal requirement could serve to supplement some existing state laws (at least as they apply to federal elections), as well as putting audits in place (and the voter-verified paper ballots needed to carry out those audits) where those requirements do not currently exist.

Sixteen states[5] have enacted requirements for mandatory manual audits.[6] At least two states *without* voter-verified paper record requirements (Kentucky, Pennsylvania) also have audit requirements. These were written into statute decades ago, apparently prior to widespread adoption of (paperless) direct recording electronic (DRE) voting systems. It is unclear whether -- or how -- these states are carrying out their statutory audit requirement, whether partially (e.g. in the few paper ballot counties) or not at all. Other states are considering audit provisions, including Florida and Oregon.

Audit selection must apply to all counties, not just some. In Arizona, the law allows party chairs to have a say in whether an audit will be conducted or not. As a result, not all counties performed an audit after November's election. A federal requirement would mandate that all counties will include at least one precinct to be audited.

Audit laws must apply to all voting systems in a state, not just some. Yet some state voter-verified paper record laws were written with a particular type of voting system in mind,

[5] AK, AZ, CA, CO, CT, HI, IL, KY, MN, MO, NM, NY, NC, PA, WA, WV. Requirements and citations of relevant legislative text http://www.verifiedvoting.org/downloads/StateManualAuditProvisions-03-07.pdf

[6] Nevada has conducted manual audits of the voter-verified paper audit trails produced by its DREs from 2% of the machines in less populous counties and 3% in more populous counties since putting VVPAT in place in 2004, but the Nevada Secretary of State's office said (in a telephone conversation) that these audits are not statutorily required. Other states, such as Vermont, have statutory language providing for discretion to conduct an audit, but where audits are not explicitly required, we did not include those states in the "StateManualAuditProvisions" document (cited above).

so the audit requirements that were included in those laws pertain just to that type of voting system. This has resulted in an ambiguous requirement for counties which may not have ended up using that type of voting system. Washington, Connecticut and New York all have laws which reference voter-verified paper audit trails (VVPATs) with DREs, and which require audits of the VVPAT. But both Washington and Connecticut subsequently adopted paper optical scan ballot systems. (New York has not yet adopted new voting systems and continues to use lever machines at this time.)

Connecticut did the right thing in November by auditing their new optical scan systems even in the absence of an update to their audit law. And they seem poised to update their statutory language in this session, as the Secretary of State has proposed a 20% audit rule, the highest percentage in the country. A bill to modify the Washington audit language to include audits of optical scan systems did not move in its legislature last session, however. Pending federal legislation would mandate manual audits that apply to *any* voter-verified paper ballot voting system, not just one type.

Most existing audit provisions specify that a percentage of precincts be audited, though some specify a percentage or fixed number of machines. The percentages range from 1% in California to 10% in Hawaii, with most around 3% to 5%. Minnesota bases its sliding percentage on population density. North Carolina's provision is unique in that it does not pre-determine a percentage of precincts, but uses a statistician to determine the appropriate quantity for each election.

Although when viewed as percentages these provisions span a wide range, workload must also be considered. There is a significant difference in workload between reviewing the entire ballot, versus reviewing just a few races. Not all states' audits require review of the entire ballot. Some examine only one contest, while others review several contests per ballot. In California, *all* contests in each county are examined. Its ballots tend to be extremely long. Thus its administrative cost is significantly greater than its counterparts with higher percentages. By contrast, Hawaii's 10% audit reviews each ballot for one contest only.

This range of state audit experiences shows that although election officials are already under significant time pressure in many jurisdictions, requirements for a 3% federal audit are administratively achievable. Audits of that approximate size (or greater) are routinely carried out in several states, and they could be adopted throughout the nation.

III. Why are audits essential?

Audits serve to identify problems such as machine malfunctions which might otherwise be overlooked. Even if, in a particular election, a problem might not affect the outcome of a race, knowing that the problem exists allows officials to correct it before any future elections can be affected.

Audits serve to confirm the accuracy of the vote count, which in turn gives voters more confidence in the integrity of the outcome, as many election officials attest:

In North Carolina, Moore County Election Director Glenda Clendenin described the audit as simple, saying it was "*no more than a clerical exercise*" and that the purpose of the hand count was "*to get voter confidence back and make sure it's right.*"[7] A Boone County paper described the hand-to-eye count as a "*test of accuracy of the machines.*"[8]

In California's San Mateo County, Registrar of Voters Warren Slocum proactively sought input and advice from technical experts to improve the audit process, including voluntarily adding absentee ballots to the audit process even before a new requirement took effect. His aim was "*to get a head start on that process because San Mateo County is aiming for the gold standard in the Manual Recount Process... establishing practices that will assure voters and election officials of the integrity of the vote.*"[9]

In Minnesota, just before implementation of the State's new audit requirement, former Secretary of State Mary Kiffmeyer said "*Audits just build confidence.*"[10] Afterward, Washington County's election director said "*When the post-election audit [requirement] was passed in Minnesota, I frankly was not a big proponent. Any local election official understands the enormous amount of work that is done by county auditors, county election staff, city and township staff and election judges. The idea of adding more duties was not appealing.*" [...] "*I was surprised at how quickly the audit went. I was not surprised by the quality performance of the equipment and our election judges... if this is what is needed to provide some assurance to those who do not have as much confidence in the system then I have no problem continuing to do the audits*," he stated.[11]

Starting in 2004, former Secretary of State Dean Heller of Nevada required election officials in all 17 counties to carry out audits of voter-verified paper records. Heller said he wanted to assure voters the results were "*the most accurate, most secure and most valid in the nation.*"[12]

Connecticut Secretary of State Susan Bysiewicz recently proposed a plan to mandate random audits in 20 percent of all precincts statewide, starting in 2008, saying, "*This is very important to ensure the integrity of the voting process going*

---

[7] http://www.thepilot.com/news/050306voters.html

[8] http://www.wataugademocrat.com/2006/0515web/primaryelectionfinalized.php3

[9] San Mateo County officials worked with VerifiedVoting.org founder David Dill, PhD, and with his ACCURATE colleague Joseph Hall and others to develop improved methods for random selection of the precincts and more secure timing and procedures. http://www.shapethefuture.org/press/2006/111706.asp

[10] Time Magazine, "Can This Machine Be Trusted?" http://www.time.com/time/magazine/article/0,9171,1552054,00.html

[11] Kevin Corbid, from electionline.org, *Case Study: Auditing the Vote* (March 2007) page 8, at http://www.electionline.org/Portals/1/Publications/EB17.pdf

[12] http://www.krnv.com/global/story.asp?s=2353009&ClientType=Printable

forward. Voters should feel confident that we have a fair and transparent election process." [13]

Audits are cost-effective. Election directors who are not already conducting audits may be concerned about the cost that carrying out an additional task of this sort will add to their budget. The principal cost of conducting audits is for time to plan, and to examine each of the selected ballots after the election, and the rate of pay for the persons required to complete the tasks.

But the cost of auditing is far from prohibitive, and in some cases is very low indeed. In a recent survey conducted by the National Association of Secretaries of State (NASS) regarding audits, one state responded that the cost --"if any"-- is borne by the counties.[14] In North Carolina's first audit after passage of their new law, when a single race was examined on ballots in 260 precincts, the average cost was $65 per precinct.[15] In November 2006, Minnesota examined three contests on ballots in 202 of its precincts, at an average cost of $135 per precinct.[16] In Nevada, an experienced election official estimated the cost of auditing 2% of all votes at about 3 cents per vote.[17] Arizona's Pima County carried out their first mandatory random manual audit since passage of their State's audit law and examined four contests each on polling place ballots from nine precincts, plus additional provisional ballots, for a little over $0.13/ballot.[18]

Labor cost is a significant variable. The rates paid to counters vary considerably due to such factors as geographic differences in pay scale. Even within the State of California, for example, one county was paying $8.00 per hour to counters and another county $18.00 per hour.[19] In Minnesota, the pay scale ranges from minimum wage to $12.00 per hour, with an average rate of about $8.00 per hour. In Arizona, a flat rate of $75.00 was paid to each counter for a process that was done within 1.5 days.[20]

Supervisory costs may be a factor, both for planning, administering and overseeing the audit process and the teams of counters and recorders. However, with few exceptions supervision is carried out by regular staff of the local elections office and during regular office hours. And except in the largest counties where dozens of contests are manually counted during the audit, the process can be completed in as little as a day or two.

An important variable to consider is the type of ballots being examined. In reviewing the time and resources devoted to North Carolina's audit process following their 2006

---

[13] http://www.journalinquirer.com/site/news.cfm?newsid=17902613&BRD=985&PAG=461&dept_id=161556&rfi=6

[14] http://www.nass.org/Surveys/Print%20Version%20-%20Post%20Election%20Audit%20Procedures%20by%20State.pdf

[15] http://www.ncvoter.net/downloads/NCSBOE_Primary_Sample_audit_count_short.xls

[16] Correspondence with Mark Halvorson, Director and Co-Founder, Citizens for Election Integrity, MN

[17] Testimony of Michael Waldman before the Senate Committee on Rules and Administration, Feb. 7, 2007, http://www.brennancenter.org/dynamic/subpages/download_file_47870.pdf

[18] http://www.azsos.gov/election/2006/general/handcount/Hand_Count_06_General_Pima.pdf

[19] Correspondence with Registrars of Voters from San Luis Obispo and San Mateo Counties, CA

[20] Audit observation report from Pima County, Arizona; Tom Ryan, AZ Citizens for Fair Elections

primary election,[21] it becomes apparent that auditing paper records printed out on thermal paper rolls from the DRE printer used there takes considerably longer than auditing paper optical scan ballots. Overall it was at least two times faster to count paper ballots than to count the thermal paper printout. In some cases as many as 8+ paper ballots could be counted per minute, versus only one or two records per minute for the paper trail printouts.

In some audit states, such as California, every contest is examined. Although the required percentage in California is 1% of precincts, the counties typically select additional precincts in order to include every contest in their jurisdiction. As an example, San Luis Obispo County (164 total precincts) randomly selected 2 precincts, but added 16 more in order to achieve the full contest range in their last audit.[22] The ballots are examined for every contest for the first two precincts, while subsequent precincts are examined only for the missing contests.

Audits called for in pending federal legislation such as HR811 would require manually counting just the federal races, in a minimum of 3% of the precincts. Especially when compared to the extensive ballot examinations a state like California has conducted as a matter of course for every election over four decades, an audit of only two or three contests presents a relatively simple investment that is well worth the effort for the resulting increase in voter confidence. The investment may also result in major savings if problems are caught in auditing and corrected before they cause a meltdown in a close election.

Audits are non-partisan; recounts may not be. Recounts can provide redress of a perceived or actual problem, while audits check to ensure the voting system is working – whether there's an obvious problem or not. Recounts are usually candidate or party-specific, geared toward "who won in this specific case", while audits are geared toward making sure the tally is correct, without regard for party or candidate. Recounts may be automatically triggered by a close margin, but if there is no legal requirement for a recount, no checking of vote totals will occur. Recounts may be requested if concerns exist (though the requestor may have to pay for the recount, which is sometimes a barrier). Mandatory audits do not have to be requested. Recounts may be initiated by candidates (in 39 states), by voters (in 18 states), and in the case of close elections (16 states). Two states (HI, MS) have no provision in state law for recounts. [23]

Despite the reasons given for the importance of doing audits, and the positive experiences of states that regularly carry out this safety-check, some may continue to perceive them as burdensome, time-consuming and unnecessary. They may see no need, if there is no immediately evident problem. Similar arguments could be made against any quality control or quality assurance (Q/A) process, yet most critical business or governmental processes have some form of Q/A, and for an obvious reason: Q/A can help prevent future problems – problems that may prove very serious and costly to rectify. Hence the

[21] http://www.ncvoter.net/downloads/NCSBOE_Primary_Sample_audit_count_short.xls
[22] Correspondence with Assistant Clerk Recorder of San Luis Obispo County March 2007.
[23] For details, see http://electionline.org/Portals/1/Publications/ERIPBrief12.SB370updated.pdf

adage, "an ounce of prevention is worth a pound of cure."

IV. Recommendations

1. Ensure the audit is readily observable and understandable by the public. VerifiedVoting.org's partner organization, the Verified Voting Foundation, in 2006 launched the first phase of a multi-year Election Transparency Project, to encourage public observation of electoral processes, including the audit process in those states where audits are conducted. In some states, audits were readily observable, while in others, observing proved impossible.

In one state, observers calling to learn the schedule of the audit were told it was done "on election night" – a plan which scarcely allows for the inclusion of observers, much less truly random selection or even pre-publication of results for comparison's sake. In another, observers were allowed but public notice was not provided – typically only party officials are notified in advance, making it nearly impossible for a non-partisan observer to participate.

By contrast, some jurisdictions went the extra mile to notify the public through press releases, posting of notice on the county website, and inviting citizen groups to participate in observing the process. HR811 appropriately requires that audits *"shall be conducted in a manner that allows public observation of the entire process,"* including the random selection process.

2. Deploy verifiably random selection of records to be audited. To ensure an equal chance at detection of problems throughout the voting jurisdiction, precincts must be selected at random. No pre-selecting, no weeding out, no setting aside, no picking the smallest ones to make for less work... Existing audit laws often fail to address the procedure for obtaining the random sample, yet to ensure confidence in the election, no one should be able to bias or predict the selection in any way. Further, observers should be able to verify for themselves the selection was random and not influenced or biased.

A motivating example of the need for verifiable randomness in the selection process was illustrated recently in Cuyahoga County, OH where election officials received felony convictions for secretly pre-selecting ballots they knew would not cause discrepancies when recounted by hand. Their goal was to avoid a lengthier, more expensive hand recount of all votes. [24]

Several California counties adopted a methodology proposed by members of the National Science Foundation's ACCURATE project which involved the public rolling of 10-sided

[24] Ohio law states that each county is supposed to randomly recount at least 3 percent of its ballots by hand and by machine. If there are no discrepancies in those counts, the rest of the votes can be recounted by machine. A full hand-count is ordered if two random samples result in differences. http://www.ohio.com/mld/beaconjournal/news/state/16536269.htm

dice to randomly generate the precinct numbers.[25] HR811 clarifies randomness with the language *"all precincts in the state have an equal chance of being selected"* with a minimum of one per county so that no county is excluded.

3. Time the selection to occur after all votes are counted and results are made public, so that results can't be "fudged" to match audit counts or vice versa. In other words, finish the ballot counting before you start deciding which ballots to check. HR811 calls for the selection to be timed *within 24 hours after the announcement* of the unofficial vote count in the state's precincts. That window, while narrow, ensures the process moves forward in an timely way.

4. The audit must be completed prior to certification of the final results, because the outcome can be affected if discrepancies are uncovered. In states with a narrow window for certification of the final election canvass, effective planning will be crucial. [One such state is currently considering legislation that would time the audit after the certification; unless the results of the hand audit can overturn certification of an inconsistent machine tally, this renders the audit pointless.] HR811 properly requires that in case of inconsistent results between machine tallies and hand tallies of the paper ballots, *the individual permanent paper ballots shall be the true and correct record of the votes cast.*

5. Minimize the time between the selection process and the actual counting to the extent possible. In states conducting audits after November 7, 2006, most carried out the selection process at most a day or two before the counting, or in some cases the same day. But in some jurisdictions, there was a delay of as much as a week or more. Such delays should be avoided, as they raise questions about what may be happening with the ballots in the meantime.

6. Include all ballot types in the audit. Several states already tally polling place ballots, absentee ballots and provisional ballots as part of the audit process. In many states, absentee voting is dramatically increasing. In California, where at least a third (and in some counties well over half) of all voters vote absentee, the audit requirement was recently changed to include absentee ballots. One county deploys a sorter to facilitate counting absentee ballots by precinct. Others sort mailed in ballots by hand prior to counting. Some jurisdictions count absentees in numbered batches rather than by precinct. Regardless of the methodology, including more than just polling place ballots in the manual audit is feasible, and very important to the process of checking the entire system for accuracy.[26]

---

[25] See http://www.cs.berkeley.edu/~daw/papers/dice-wote06.pdf "The Role of Dice in Election Audits," A. Cordero, D. Wagner, D. Dill, June 16, 2006 for more on random selection methods and practices.

[26] With the convenience to voters of absentee ballots comes concern about security, including how to track chain of custody of such ballots. A mechanism for tracking ballots the way other mail is tracked could help ensure the ballots reach their destination.

8. Prepare a plan in advance for how to investigate and handle discrepancies, and publish the plan. States and counties should also publish the results of the audit, including discrepancies noted, and how those discrepancies were addressed and resolved.[27]

9. Establish a requirement for broader audits if unexplained discrepancies are found during the audit. Doing an audit but ignoring problems that are uncovered defeats one of the primary purposes of the audit, i.e. ensuring the accuracy of the election results. Very few states have rules to trigger wider audits. If problems are uncovered during an audit, the next steps should not simply be left up to the discretion of election officials without written procedures governing those steps. Even a small discrepancy can, if projected to a full audit, potentially alter the outcome of a contest. Identifying the threshold for escalation of the audit to a wider area (e.g. additional precincts, up to and including all precincts if needed) is an essential part of the audit procedure.

VI. Conclusion

Audits are critical to our democratic process. Properly conducted audits offer multiple benefits: increasing election transparency, promoting public confidence, reducing disputes, protecting election officials from unfounded criticism, ensuring accuracy, improving the conduct of future elections, and creating a feedback loop that allows us to assess what is working and what isn't working.

Audits are feasible and cost-effective. They already being done well in some places, but they are just not being done in enough places. We know problems will occur in every election, particularly with new technology in many jurisdictions. Audits allow us to uncover and correct problems as they arise and carry out continuous improvement of the electoral process.

Voter-verified paper ballots are necessary for audits to be meaningful. No voting system should be used for our elections unless it is auditable. Today, the only way to ensure our elections are auditable is by using voter-verified paper ballots. Congress can help make our elections more transparent and reliable by passing a federal requirement for voter-verified paper ballots and mandatory random manual audits, taking into account the nine recommendations provided herein. Thank you.

---

[27] The list should include everything, not just discrepancies that officials could not explain. A good example can be found in North Carolina's audit reports.
http://www.ncvoter.net/downloads/NCSBOE_Primary_Sample_audit_count_short.xls

Ms. LOFGREN. Thank you very much. This is very interesting and useful, and as I was listening, I was thinking about the years I spent on the Santa Clara County Board of Supervisors when we had elections that we were in charge of, and it always ended up that we were the last to be counted, I think, in the State of California because we were so cheap about new equipment, but none of us at the time really ever considered that it would be inaccurate. It is only as elections have become closer and closer that we realize that the technology—you know, that there is no 100 percent, and it is something that most of us really were not aware of and that we did not focus in on, and really, although when it comes down to a recount situation and one side is going to lose, you know, you see partisan issues, and it is just a normal part of American life. But the fact is, if there is a defect, it can benefit or disadvantage either party. So, you know, I am willing to run an election and either win or lose. What I want to make sure of is that the people who are making the decisions are the voters, not anyone else, and that really gets to the question of these voting machines because we cannot see it in the same way, and Mr. Ehlers is right. I mean, there is a history. You can defraud the electorate with paper ballots, too, and we know historically there have been times when that has happened, and that is wrong, but the concern about the machines is that you would not even know it, and so here is the question.

Ms. Hoke, you mentioned in the audit—and I am not familiar, really, with the audit—that there were software issues, that there were hardware problems. Can you briefly describe what those issues were and how we could set a standard to avoid something like that?

Ms. HOKE. Yes, Madam Chairman, I would be happy to.

The software issues—I apologize for my phone. I should have turned it off.

Ms. LOFGREN. It is a beautiful sound.

Ms. HOKE. It is about to quit.

The software situation is that we specifically requested, using generic terms, the electronic files that we needed to be able to compare in with the DRE machine totals, meaning the long reports from the DRE units and the optical scan totals. Those files were not made available to us although I had stayed up 36 hours to catch the files at the conclusion of the election.

So, as it turned out, the IT and Ballot Department managers said that the files that we needed did not really exist. After a long series of discussions—and we still do not know whether a singular file exists, since we do not have access to the Diebold information. We ask: what is possible to obtain? What files are created? Were there really two usable files that local officials simply did not tell us about? Was it that the software does not produce files that make it easy to audit? We do not know the answer, but we were told that we would need a whole range of files and that we would have to take file A and back out the data from file B from file A, and it was a complicated series of steps to end up with a number that then we could compare against certain precinct totals.

One of the reasons that we very much need a supervisory authority who has access to the—shall we call it—I do not agree with

"proprietary information" but, to whatever degree it is, for the authority to be able to study what files should be made available that are appropriate for the audit, that mandate at what time during the tabulations those files will be saved, and then produced at what time. We must have been at the Board of Elections five different times just on a mission to obtain the electronic files. That is a problem.

As far as the hardware, the optical scan devices of at least the two major election vendors do not count ballots, optical scan ballots. They only count ballot pages, which means that it is not possible simply by feeding thousands of ballot pages through a scanner to know how many ballots have actually been counted. It is a separate step that must be undertaken. It is perhaps a hardware design issue plus software issue for us to be able to report accurately how many ballots were counted.

Ms. LOFGREN. Mr. Norden, you have been with the Brennan Center for a long time and have looked at these technology issues. Do you have recommendations for us to address the kind of issues that have just been described?

Mr. NORDEN. Well, one of the things I would say that would be very helpful, particularly in terms of problems with software that we have seen, is that there are often problems in aggregating votes from a number of machines—and this has occurred several times in the aggregation tally software. So one of the things is that there are additional kinds of audits that we can do and that many States do that will ensure that, number one, we are deterring any kind of attacks against the voting system but, more importantly, that we are detecting the kind of errors that might cause us to get wrong tallies.

So, for instance, one of the things that they do in California and that they do in New York and several other States—Texas—is there is a reconciliation process to ensure that we look at the vote totals that come out of the precincts from the machines and compare them to the tally server totals, and make sure that what happened at the tally server, the totals of what the tally server are giving us, are correct. That is a check against the software there.

Another is making sure that the number of voters who signed in to vote is relatively close to the number of voters who the machines are telling us who voted. In the end, it is unavoidable, given the amount of software that these machines run on and the many sources that they come from, that we are not going to sometimes have problems with the software. The key, I think, is to make sure that we are making the appropriate checks and reconciliations that are necessary.

Ms. LOFGREN. My time has expired, so I will turn to Mr. McCarthy.

Mr. MCCARTHY. Well, thank you, Madam Chair.

This has been a great hearing. I mean, I appreciate all of the input everyone has given.

Doug Lewis, you are the executive director of the National Association of Election Officials. Is that what all of the secretaries of state belong to?

Mr. LEWIS. It is all of the election officials from townships, cities, counties, and States.

Mr. MCCARTHY. Okay. I was reading your 8-page one here. It is very thorough. You are giving us some different ideas. My question is: Did you look at this based upon—you wrote a lot of this about H.R. 811. Did you look at any timeframe of what that would do to the Electoral College?

Mr. LEWIS. I think it is a legitimate question here.

The truth of the matter is we saw in election 2000 that the electoral college had to meet before we could actually finish a recount. If we are going to add in and layer on an audit procedure that is a multiple audit procedure of multiple levels, I think we are really looking at some point in another close presidential election that we may not be able to actually get to it and get it done by the time that the electoral college is going to meet. So it seems to us that it is a question that you all have to think about. You have to look at this as to what your desires are and also recognize that you then make it impossible to get to the point that the public knows who won.

Mr. MCCARTHY. Thank you.

Pam Smith, I was reading yours, too, here. You said, on page 2, procedures should be defined governing what to do, in essence, saying that paper should be the final on the audit; is that correct?

Ms. SMITH. Yes.

Mr. MCCARTHY. Now, were you here earlier for the last panel?

Ms. SMITH. Yes.

Mr. MCCARTHY. We had an individual from Ohio who raised a very good point where he had the VVPATs, the DREs, and the paper did not come out to be the same as the computer; whereas, the computer came out with the right number of the number of people who voted, but the paper, knowing that we have people who are going and feeding the paper who do not do this every day for a living, got jammed. And the computer was right, and the paper was not, and his opinion was different than yours. I do not know if you could give me a little elaboration on yours.

Ms. SMITH. Sure.

I think we have to think of this not just in terms of DREs and VVPAT-type paper trails but in general. You have a computer record that voters never get a chance to see, and you have a paper record that they can confirm is accurate. Now, in the case that he cited, his very smart poll workers were able to redirect the voters so they were voting on the machine so they could check the paper.

Mr. MCCARTHY. So you would say they were right in what they did?

Ms. SMITH. Yes, that was absolutely right to redirect the voters so that they could have an opportunity to check on paper.

Mr. MCCARTHY. And they were able to do that because the machine showed it?

Ms. SMITH. In that particular case. In some cases, the machines may not tell you, and the voter may not know. They may not have been advised that you really should check this paper record because this is the hard-copy record of your vote. Make sure it is accurate. That is something—that notification, I think, is part of that, H.R. 811. You need to—if you are expecting voters to use a new system they are not familiar with, you have to guide them somewhat.

Mr. MCCARTHY. Should you mandate one over the other as being the final tally?

Ms. SMITH. Say again?

Mr. MCCARTHY. Should you mandate paper or the computer to be the final tally, one over the other? I mean——

Ms. SMITH. I think you can only mandate to be the final arbiter of the voter intent the document that a voter has had a chance to look at.

Mr. MCCARTHY. Okay.

Ms. SMITH. If they do not get a chance to look at it, which is true about computer bits and bytes in the ether, then they cannot confirm that that is right.

Mr. MCCARTHY. Okay.

Lawrence, you and Pamela talked about—was it Pamela? No, it was Candice. You talked about post-election—is that correct?—that voters do not feel that the elections are being held honestly or they have questions as to the honesty of the elections; is this right?

Mr. NORDEN. I think, unfortunately, that there is certainly a large segment of the population that—and I think it is incredibly corrosive to our democratic system—do not have confidence in the results of elections.

Mr. MCCARTHY. Just because my yellow light is on, if you have any polling on that, if you could show me—because the executive Director of the National Elections cites CNN says 88 percent in the last one, but you looked at all of the phrases—I guess Pam did. In all of the phrases of auditing, have we ever talked about when we are auditing this election on auditing who actually votes? Has anyone brought that up? Because it seems like, okay, we are auditing the people who voted, but have we ever checked from the very beginning that the people who did vote were the individuals who have the right to vote? If not, would you propose that in legislation for identification? Anybody? Yes.

Ms. HOKE. There is a kind of reconciliation or audit process as far as checking to see whether the—at least in Ohio—about the number of people who signed in versus the number of votes. There have been some additional studies from time to time to ascertain whether people did have their IDs checked, and in Cuyahoga County, we did do a further study—I do not have the results on that, but I will try to obtain that data for you if you would like. This concerned whether people's IDs were properly checked and, therefore, valid voters. I will try to provide that.

Mr. MCCARTHY. Because the only thing—I know my time is up. If it is true the voters do not believe whether it is true or not, if we are going to audit in the end, which in some way we do need to have checks and balances, we also need to check and balance who actually went there.

Mr. NORDEN. Well, one point I would like to make, Congressman, is that—and a point I tried to make earlier is that, at this point, there is near universal agreement among computer scientists and security experts about the security vulnerabilities of these machines.

Mr. NORDEN. I am certainly happy to have the Brennan Center come back and talk about allegations of individual voter fraud and issues of voter ID, but there are two things I can say about that

issue for certain. One of the things we looked at in our security report is that the number of votes that could be affected by problems with the voting machines dwarf in comparison to the number of votes that could be affected by any kind of retail voter fraud that you are talking about. And the second is we do not have that same kind of consensus at this point about whether or not there are instances of voter fraud, individual voters who are not entitled to vote who are coming to vote.

Ms. LOFGREN. The time has expired.

I would note that we have all been handed that report, which we will make part of the record.

Ms. LOFGREN. Now, Mr. Holt, it is your opportunity to ask some questions.

Mr. HOLT. Thank you, Chairwoman Lofgren and Ranking Member McCarthy. Thank you for allowing me to join you. Thank you for holding this hearing for the legislation H.R. 811.

I know there has been a lot of talk about the security and accessibility of equipment and the openness of software and any number of other things, but the heart of the legislation is the auditability and the use of that auditability, the audit, itself. There are too many unresolved irregularities hanging out there that are really undermining our belief in our ability to govern ourselves, and as I often say to middle school students and others, self-government works only if you believe it does. I think there is a lot that has shaken that faith that we need to address, and so at the heart of the legislation are routine, random, independent audits, and this concept, certainly, has been endorsed by many organizations, including some represented here today, and I think the specifics have been examined. The specifics have been examined and, in many cases, endorsed as well.

Ms. Hoke or Mr. Lewis, let me ask you: Do you think that the proprietary software printout at the end of the day after the polls are closed would satisfy your definition or a reasonable person's definition of an "independent audit"—and "independent auditability"—I beg your pardon—and then whether that would, by itself, count as an audit?

Ms. Hoke.

Ms. HOKE. We took a position in Cuyahoga County that an audit would not be sufficient unless independent. Part of the reason—I mean, our audit report should be available probably within the next 10 days, and you will have some very important data that will show that it is important to get underneath the tabulation software's, shall we say, massage of the numbers to find out what the real raw data are. You may find that there are differences between the raw data and what is actually reported by the software program. It was our view that it is important to know that.

Now, it may be that that is a software design problem that could be corrected, but certainly, our software engineers who are working with our audit felt quite strongly that this is one way to discover whether there is rogue code in the tabulation server or in some place other than the voting devices themselves that could cause the report of the election results not to match the real raw data, and so we very much wanted that raw data. And we did do a study of

only three races, and we found that there were differences between the two election results tables.

Mr. HOLT. Mr. Lewis.

Mr. LEWIS. Congressman, I will say to you that there has not ever been at this point one verifiable circumstance in which anybody has been able to show that electronic voting has been manipulated.

Mr. HOLT. That is not what I asked.

Mr. LEWIS. I understand.

Mr. HOLT. That is not at all what I asked, because there are very many documented unresolved irregularities. I can list 15 counties off the top of my head. So, clearly, what I asked is, does a software printout at the end of the day constitute auditability, in your mind?

Mr. LEWIS. If you look at the international standards that are created for computer memory in terms of storage—and all of these systems have at least a double redundancy and most a triple redundancy in terms of their memory and storage of ballot images that are retained within the system meeting the Federal voting systems guidelines. If you look at that, those standards are far higher than the standards for paper ballots. We can faithfully reproduce the votes as the voters voted them from the Ballot Image Retention. We can show you a ballot image of how every voter voted.

Mr. HOLT. Of how every voter voted or——

Mr. LEWIS. Ballot image retention is required by Federal voting systems guidelines, for all electronic equipment, and so you have double and triple redundancy there to where you can pull that out there. Yes, sir, I think you can show with great veracity that it is exactly what the voter voted.

Mr. HOLT. I think a key point is your statement that this shows how every voter voted, and I think you have missed, if I may say with respect, a basic point that every computer interface organization has addressed that the machine cannot verify itself. It is a fundamental principle with computer science.

Ms. LOFGREN. Our time has expired, and indeed, the panel has been very helpful, and we thank you for the time invested here with us. It is important. We will keep the record open for 5 days. We may have additional questions for you, and—yes, sir.

Mr. LEWIS. I want to clear up, on page 8 of my testimony, a technical—I misstated one number incorrectly.

Ms. LOFGREN. If you will get it to us, we will make that correction, sir.

Mr. LEWIS. Okay. Thank you.

Ms. LOFGREN. Thank you, again, very much for the time you have spent and the expertise that you have shared with us.

The hearing is adjourned.

[Whereupon, at 4:35 p.m., the subcommittee was adjourned.]

[Information follows:]

Collaborative Public Audit

of the
November 2006 General Election

pursuant to the charge from the
Cuyahoga County Board of Elections

Final Report – Submitted on April 18, 2007 by

The Collaborative Audit Committee

Democratic Party of Cuyahoga County
Leslye Huff, J.D.
Amos Mahsua, C.P.A.
Republican Party of Cuyahoga County
Gordon Short, J.D., C.P.A.
League of Women Voters
Kathy Woodbridge (Cuyahoga Area)
Kurt F. Miller, Ph.D. (Shaker Heights)
CASE-Ohio (Citizens' Alliance for Secure Elections)
Ron Olson
Dan Kozminski
Greater Cleveland Voter Coalition
Roslyn Talerico
Joyce Porozynski

Coordinator

The Center for Election Integrity, Cleveland State University
Candice Hoke, J.D., Project Director, Public Monitor
Abigail Horn, M.A., Audit Coordinator

Audit Methodology and Statistical Analysis

The Northern Ohio Data and Information Service (NODIS)
Ellen Cyran, M.S.
Mark Salling, Ph.D., Director, NODIS

Table of Contents

Introduction

As is true of many initial audits, whether of a for-profit company or public agency, this Audit Report relates both "good news" and "bad news." While some readers may emphasize the bad news, we believe the overarching message should be that the Cuyahoga Board of Election's authorization for the November 2006 election audit is itself crucial good news about the agency's prospects for moving forward decisively.

We – the Collaborative Audit Committee and the coordinating Center for Election Integrity – strongly affirm that independent audits provide information to a public agency that will allow it to move forward with clear knowledge of its successes, and also of problems that need to be rectified. In the election context, audits permit the identification of problems with election managerial systems or technology, such as with voting machines or tabulation equipment, and thus allow an agency such as a local election board to develop an effective action plan for improvement. An election agency's adoption of a practice of full disclosure about (1) its efforts to identify successes and problems fully and impartially, and also (2) its plan to correct the problems, is ***the path*** toward rebuilding the public's respect and trust in reported election results.

Proposals to audit elections may raise internal objections because problems may be discovered that otherwise might remain hidden. But the absence of election audits works to both the agency's and the public's disadvantage: problems may remain unknown and uncorrected, and questions or charges about election accuracy continue, reducing public confidence in the agency. Any staff efforts expended to conceal problems not only wastes energies and reduces public confidence, but also means that when the problems do surface eventually, sometimes in a particularly injurious manner, the agency may be shaken to its foundations. Better, we believe, to discover the areas of success and those of needed improvement, and deploy resources to improve.

With the support of major political party county organizations, the Cuyahoga Board of Elections authorized this audit, for which we believe it deserves public recognition. While the Audit participants did encounter impediments and delays to the auditing process, we believe that even these provided opportunities for learning more about the administrative, technical, or legal changes that need to occur to smooth the process for auditing elections as a routine matter.

Even though this election audit cannot provide conclusive results on e-voting device accuracy, and could not be completed in the expected time frame because of a wide range of local managerial issues, we believe it provides an important first step toward election auditing in Cuyahoga County and in Ohio. We hope that this Audit Report will assist the Ohio Secretary of State, all Ohio local Boards of Election, election reform organizations, and other election officials nationwide in seeing how an independent audit process can be created and function at the local level. Additionally, we hope the public will recognize that this Report contains the kind of information that all election administrative agencies need to better achieve the public charge for producing accurate election results and to facilitate sound improvements in election administrative practices.

Executive Summary

An independent audit of the *unofficial* count of the November 2006 election in Cuyahoga County was undertaken collaboratively through representatives[1] by both major political parties and a number of election reform organizations. Cleveland State University's Center for Election Integrity and the Northern Ohio Data Information Service coordinated the audit process and technical services, and also supplied methodological guidance and statistical analysis.

The representatives of the organizations, and the volunteers assisting, conducted two collaborative audits. They are described here along with some terminology that will be useful in understanding the audit results.

♦ A random sample of election reports from DRE touch screen voting machines was compared for consistency with the report of precinct election results from the GEMS tabulation computer.

- The DRE voting machine produces a "Long Report" after the election has closed with vote counts for each race/issue in each precinct.
- The central ballot tabulation system software is named GEMS. The GEMS tabulation reports provide election results.
- The SOVC Report is the comprehensive Statement of Votes Cast report from the GEMS server. It shows the total votes cast for each candidate and issue by precinct.

♦ A hand count of a random sample of absentee or "early voting" ballots was compared for consistency against a GEMS report of electronically tabulated election results.

- Early/absentee ballots are optical scan paper ballots with voter selections marked on the ballot by the voter.
- These ballots are read by an optical scan reader and with the voting information transmitted into the GEMS system.

This audit did not evaluate: internal controls of the CCBOE; security procedures or chain of custody for the Long Reports; or the consistency of individually cast DRE ballots with the totals recorded on the DRE unit's Long Report. Additional audit procedures would be needed to evaluate these areas and were beyond the scope of this audit.[2] For a complete explanation of all the findings, please read this entire report.

Selected Findings

A. DRE Touchscreen Voting Machines: Audit of the "Long Reports"

Conclusion One There is a high probability that the DRE Long Report (precinct) results match the GEMS produced election results published on November 8, 2006.

[1] For the list of individuals and their credentials who participated in the Audit Committee, see the cover page. For further background on the authorization of the audit, see Appendix 1.

[2] The impediments posed by Ohio state law to more complete auditing are discussed at II. B and III. B.

Recommendation: We recommend that a random, independent audit of the election results be performed before CCBOE certifies the election. (See Top Tier Recommendation #1 *below*).

Conclusion Two Expecting a complete set of DRE Long Reports with all data clearly recorded for all precincts currently is not realistic.

Recommendation: As part of the planned security review, the CCBOE should assess the viability of using Long Reports as part of their overall security plan, and should take into account in selecting voting systems the ability to achieve full verification of the accuracy of election results.

Conclusion Three A number of DREs had been vendor-marked with non-unique serial numbers; several pairs of DREs were identified within the sample as having serial numbers duplicated in other DREs owned by CCBOE.

Recommendation: Resolve the non-unique DRE serial number problem by taking a number of actions with Diebold and internal tracking of serial numbers.

B. Optical Scanning: Audit of "Early Absentee Ballots"

Conclusion One Election result data in the GEMS report corresponded closely to the results obtained by the audit hand count of the optical scan ballots.

Conclusion Two The sorting process for early absentee optical scan ballots into precinct batches prior to scanning was neither complete nor accurate.

Recommendation: Hand sorting into precincts and batches should be replaced by a more automated system with appropriate quality control measures.

Conclusion Three There was a very low frequency of discrepancies that appears to be caused by a scanner misreading of some of the optical scan ballots.

Recommendation: An audit similar to this, comparing electronically recorded optical scan results to those obtained by hand-counted examination of the optical scan ballots, should be performed after every election and before certification.

Conclusion Four Some ballots were apparently scanned for the tabulation at one point but were not included in the GEMS elections results or on the SOVC, probably because the ballot batch had been deleted (because of flawed data) and then was not rescanned.

Recommendation: Deletion of ballot batches must have greater quality control to ensure re-scanning of the deck.

Conclusion Five Some ballot batches were scanned twice producing a double-count of those ballots and their votes.

Recommendation: The electronic identification of an optical scan ballot batch should be unique and constant; and greater quality control measures need to be introduced to ensure all ballot batches are counted only once.

Conclusion Six The electronic identification of a ballot batch may change within the scanning process and between scanning events, reducing the ability to accurately track that the ballot batch has been counted, and counted only once.

Recommendation: A mechanism should be developed to record and track batches of ballots with appropriate quality control measures.

C. Security, Accuracy, and Sufficiency of the Data Needed for Auditing

Conclusion One The CCBOE's lack of compliance with its own electronic and physical security policy is unacceptable.

Recommendation. An independent assessment of the security policy's adequacy and its implementation within the CCBOE should occur.

Conclusion Two Some indicators of *possible* database corruption were identified in an initial database integrity evaluation.

Recommendation: The CCBOE should initiate an independent evaluation of the GEMS tabulation database by a qualified consultant to ascertain whether database corruption occurred in the November 2006 election.

Top Tier Recommendations for Systemic Improvement

1. Independent audits should become a routine part of the election process.

Independent auditing is standard business practice and should be applied to our election and voting systems because of their importance. A reasonable approach might be to perform a professional or other independent audit after each major election and a collaborative internal audit after smaller local elections. The time and cost involved do not need to be exorbitant and will decrease as problems are resolved and process controls put in place. The audit should occur prior to certifying the election.

Although this audit found a relatively small number of ballot batches that had been miscounted in the unofficial optical scan count, the audit identifies problems that indicate proper procedures for tabulation accuracy were not consistently followed. Institution of routine independent audits will facilitate tabulation accuracy, and administrative and technical improvements, and thus demonstrate to the public that confidence in the election process is well founded.

2. Reconsider the feasibility and wisdom of supporting two major voting systems: optical scan and DRE touch screens.

The problems found in this audit, the Election Sciences Institute audit of the May Primary, and report from the Cuyahoga Election Review Panel (July 2006) call into question whether it is practical and cost effective for Cuyahoga County to support two voting machine systems (i.e., electronic and optical scan). Some factors to be considered include:

- Election costs for 2006 substantially exceeded the budget allocated;
- It is unclear if DRE electronic voting can support the turnout in a Presidential election;
- CCBOE staff must be hired and trained to support both systems, and have not reached high performance standards in managing either system; by focusing on one system higher performance standards can likely be met more quickly.
- The DRE devices present considerably greater hurdles to cost-effective and complete auditing than do paper optical scan ballots.

3. A comprehensive evaluation of the election database should be undertaken by qualified technical professionals who are independent of voting system vendors.

Some indicators of *possible* database corruption were identified in an initial database review but were not investigated despite the Monitor's repeated urging. In an independent evaluation of the GEMS official results database the task should be:

- to ascertain whether database corruption occurred in the November 2006 election database,
- and if so, to determine the scope and impact of any corruption for the tabulated and reported results; and
- in light of Microsoft warnings, to provide recommendations on how to avoid tabulation database corruption to the maximum extent feasible, delineating the steps to be taken to protect election data as tabulations are occurring.

Glossary of Terms Used

Absentee voter: Voters who cast their ballots before Election Day, by mail or in-person at the Board of Elections; they do not vote at a precinct polling place.

Absentee audit: An audit of the optical scan ballots used by absentee voters.

Batch: The digital representation of a scanned deck (or decks) of optical scan ballots as recorded by GEMS.

CCBOE: As commonly used, this term can confusingly designate either the *agency* that conducts elections in Cuyahoga County -- the Cuyahoga County Board of Elections—or its four-member governing *Board*. In this Audit Report we use CCBOE to refer to the agency as a whole, which includes its staff as well as its governing Board. The Board is comprised of two Republican and two Democratic members who normally are nominated by the local major political parties and then formally appointed by the Ohio Secretary of State.

CAC: Collaborative Audit Committee—the representatives of the two major political parties and three election oversight and advocacy organizations (see cover page) who composed the policymaking arm of this Audit.

CEI: Center for Election Integrity of Cleveland State University, which was appointed to serve as the Public Monitor of Cuyahoga County election reform by both the Cuyahoga Board of County Commissioners and the Cuyahoga County Board of Elections.

CERP: Cuyahoga Election Review Panel. The Panel was appointed by the Cuyahoga County Commissioners and the Board of Elections to review the 2006 Primary Election and make recommendations for improvement. The Panel published a final report on their findings, known as the CERP Report (www.csuohio.edu/cei/).

CSV file: Comma Separated Values file; a file format used for data files that permits them to be read on a variety of computers.

Deck: The electronic representation of a batch of optical scan ballots that will be scanned together and whose votes will be reported to the GEMS database as a unit.

DESI: Diebold Election Systems, Inc. the subdivision of Diebold, Inc. that manufactures and markets election voting systems and technical consulting services. Cuyahoga County uses Diebold's

DIMS: This is the software program Diebold Election Systems markets for recording voter registrations, processing absentee ballot applications, evaluating candidate or issue petitions, and managing poll worker information (It is the acronym of Data Information Management System). The Cuyahoga CCBOE uses DIMS in all of these ways. DESI materials note it interfaces "seamlessly" with the GEMS election tabulation software but this interface has been highly problematic in our County.

DRE: a type of electronic voting machine where the machine electronically records voters' choices (Direct Recording Electronic). In Cuyahoga County, the DRE model that is used is a Diebold AccuVote TSX with VVPAT printer. This DRE is a "touchscreen" where the computer monitor shows the ballot, and the voter "touches" rectangular boxes shaped to look like buttons to simulate the pushing of a button under a ballot choice. Most of Cuyahoga County voters currently vote on DREs at the precincts on Election Day.

EAC: U.S. Election Assistance Commission. The EAC was established by the Help America Vote Act (HAVA). It disbursed federal funds to States for replacing their voting systems. Currently, the EAC's prime task is to facilitate election administration improvements. It serves as a national clearinghouse and resource for information pertaining to the administration of federal elections, including for the technical aspects of voting systems.

EDT: Election Day Technicians, a special poll worker position created by the Cuyahoga CCBOE to activate and manage the DRE touchscreen units at polling locations.

Election certification: Formal approval of the CCBOE is required to officially confirm the results of an election. The date for certification is established by Ohio statutes.

ESI: The Election Science Institute is a nonprofit, nonpartisan election management-consulting firm located in San Francisco that was retained by the Cuyahoga County Commissioners in April 2006 to evaluate the accuracy of the DRE touch-screen voting units. ESI conducted an audit of the individual printed ballots cast on DRE units in the county's May 2006 Primary election.

E-voting: refers to "electronic voting." While the term is somewhat contested as far as its scope, generally it refers to any device on which voters cast ballots, or any election system where the reading, recording or tabulation of votes cast involves computers.

Flash memory: Internal computer memory within each DRE touch-screen unit, which stores election, results until erased. Votes cast on the electronic voting machines are recorded in two places: 1) the memory cards that are inserted before the election and removed after the election for counting, and 2) in flash memory located on a computer chip which remains inside the voting machine.

Firmware: Vendor-installed operating software.

GEMS: this is an abbreviation for a computer software program (Global Election Management System) that Diebold Election Systems sells for the creation of electronic and paper ballots, and to serve as the central tabulation program for recording and counting votes. The Cuyahoga CCBOE uses GEMS in all these ways.

Long Report: From the DRE units, a paper printout of the summary election results (votes sorted into candidate and issue, presented by precinct) for all the ballots that were cast on the one DRE voting machine from which the printout was generated (from an integrated printer).

Memory card: A removable electronic disk similar to a "floppy" that records the votes cast on a DRE voting machine. In Cuyahoga County, the memory cards are inserted into the electronic voting machine before the election, removed at the end of the election, and delivered to the

CCBOE where the voting data are uploaded to GEMS to count the votes cast on the DRE machine and recorded on the memory card.

NODIS: Northern Ohio Data Information Service, the regional data center located at Cleveland State University. NODIS provided statistical and other professional support for the Collaborative Audit.

Optical scan ballot: A paper ballot, which in November 1006, was divided into three columns. The ballot lists each race or issue with ovals beside each voting choice. To cast a vote that can be accurately read by the counting machine ("scanner"), the voter colors in the oval that reflects the voter's choice.

Optical scanner: The computerized device used to read and record the votes marked on paper ballots ("optical scan ballots"). Each scanner is connected to the GEMS computer by a wired network, where the GEMS program tabulates and reports election results.

PDF file: Portable Document Format, a type of file format.

Precinct: A geographic subdivision of a county, town, city, or ward for election purposes.

SOVC Report: The comprehensive Statement of Votes Cast report from the GEMS server. It can show the total votes cast for each candidate and issue by precinct.

VVPAT: By Ohio statute, every DRE unit must be equipped with a printer that will produce for the voter's review a Voter Verified Paper Audit Trail. The VVPAT is the printout of each voter's selections. After it prints, the voter must push a button affirming that this is the VVPAT correctly presented the voter's choices in order for the ballot to be officially cast and counted. The VVPAT is the official legal ballot of voters who vote on DRE units in Ohio.

FULL REPORT

Collaborative Public Audit for Cuyahoga County

I. Background: Achieving Independent Verification of Election Results

Achieving accuracy in reported election results is a primary objective for any quality election administration. Given the range of recent information reported nationally about possible problems with e-voting technologies, and also some of the problems the Cuyahoga County Board of Election (CCBOE) experienced in prior elections, local election reform organizations and the major political parties sought to have the county's election results independently verified as accurate reflections of the ballots cast in the November 2006 election. In early fall, the chief initial public concerns focused on the DRE touchscreen voting devices which were to be used at polling places on election day.

After discussions with election reform organizations about their concerns, the Public Monitor of Cuyahoga Election Reform[3] introduced at a Board of Elections public meeting a proposal for a Collaborative Public Audit. The proposal pledged that the Monitor would seek the cooperative involvement of the local Democratic and Republican Parties, plus several election reform organizations to conduct the independent audit. The proposal also requested the CCBOE to send a representative to the audit-planning group.[4] Per the reform organizations' requests, the audit was to focus on the Diebold DRE touchscreen voting machines that are primarily used in Cuyahoga County for Election Day voting at the polling locations. Later, by political party request, the audit was expanded to encompass the optical scanning operations.

→ ***Further background information on the process for obtaining authority to conduct the audits, and the participants and governing structure, can be found in Appendix 1.***

The Collaborative Audit participants believe the public deeply desires independent verification that the election results that the e-voting technology has generated are accurate. We additionally suggest that both the election administrative staff and the public at large need to know whether the voting machines' programming maintained its integrity after the machines passed the pre-election testing and were deployed to the polling locations for Election Day. Reliable information on these and other questions are crucial so that sound decisions can be made as to the voting and database technologies we used and so that any corrections in administrative or other systems that are needed can be identified.

We believe that yet another reason led to broad support for election auditing in our county. Our local and statewide election reform organizations (and perhaps also the county political parties) supported the initiation of election auditing to increase incentives for the administrative staff effort to reach higher standards of tabulation and reporting accuracy, and to deter the prospect of

[3] The Center for Election Integrity of Cleveland State University per a proposal and testimony prepared by its Director, Candice Hoke.

[4] After numerous requests for a representative or liaison who would serve as a non-voting member of the Audit committee, the CCBOE Director declined to authorize a representative.

tampering. The thought was that CCBOE managers would desire the independent audit "report card" to be a positive report regarding the accuracy and management of the election.

A national Election Audit Workgroup teaming the Brennan Center with the Samuelson Law, Technology & Public Policy Clinic at Boalt Hall School of Law (UC Berkeley), as well as several election officials and leading academics has been working to evaluate current audit laws and procedures, and to provide critical analysis to public officials as they begin to adopt audit schemes and procedures. The Workgroup has thus far identified five core goals that should motivate the design of election auditing: increasing public confidence in the results of an election; deterring fraud against the voting system; detecting large-scale systemic errors; providing feedback that will allow jurisdictions to improve elections and machinery in future years, and confirming to a high level of confidence that a 100% manual recount would not change the outcome of the race.

We agree strongly with this statement of election auditing design goals but would add a sixth: providing additional incentives for the staff to reach higher standards of accuracy. In order to achieve these six and other auditing goals, we have concluded, as has the Election Audit Workgroup, that the independence of the auditing entity is essential.[5]

Largely because of the unexpected impediments to election auditing that the Cuyahoga effort encountered, this audit might best be considered a pilot program for identifying the necessary procedural or informational components that must be in place in order to conduct an effective audit of two different types of voting systems. Some of these components can be achieved by local Board of Election policy and procedural changes but others will likely require the Secretary of State's action. Still other impediments exist because of State statutory law but this audit may assist in identifying the legislative action that would be warranted.

While the audits that were conducted are limited rather than comprehensive and conclusive on the questions of accurate tabulation of election results in November's election, the information acquired should be useful for achieving the other election performance and auditing goals identified above.

The Collaborative Audit Committee would like to thank the over forty volunteers that gave their time over numerous days to help conduct this audit. Without this huge volunteer effort, this audit would not have been possible. We also commend the Cuyahoga Board of Election for taking an Ohio leadership role in initiating election auditing and thus creating an independent mechanism for verifying the announced election results.

[5] Lawrence D. Norden, Statement to the U.S. House of Representatives, Committee on House Administration, Subcommittee on Elections, March 20, 2007 at 2; Candice Hoke, Statement to the U.S. House of Representatives, Committee on House Administration, Subcommittee on Elections, March 20, 2007 at 2 (this testimony to the Subcommittee on Elections that held hearings on Federal Election Auditing can be found at http://www.verifiedvotingfoundation.org/article.php?id=6445).

II. DRE Touchscreen Voting Machines: Audit of the "Long Reports" as Compared to the GEMS Tabulation Computer

A. Background

On Election Days, most Cuyahoga County voters now cast their ballots on an electronic voting device called a "DRE touchscreen." This device allows voters to read their ballot on the computer screen and push buttons on the screen to register their voting choices. At the end of choosing their voting choices, the DRE produces a summary page on screen to allow the voter to check to see whether the machine has recorded the individual's votes correctly. The voter can choose to return to earlier pages and change a vote. (Technically, a DRE voting device is a "direct recording electronic" voting machine that maintains an internal computer chip memory of ballots cast as well as records the same data on a removable memory card.) Cuyahoga County owns approximately 6,000 Diebold DRE voting devices.[6]

How and why "Long Reports" are produced. Ohio statutory law requires that all DRE units produce a "voter verified paper audit trail" or VVPAT. When a citizen uses a DRE touchscreen to vote, the unit prints for the voter's review a list of the ballot choices the voter made so that the voter can verify his or her vote before pressing a button that essentially means "yes, the printout of my voting choices is correct; count this ballot as is." The paper on which this statement of voting choices is printed is called the VVPAT.

Cuyahoga County has administratively organized its elections so that all the DRE units in a voting location (for instance, a school gym) can be used by voters from any precincts assigned to that location. The poll workers are trained to encode the "voter access card" so that the machine will bring up on screen the correct ballot for the precinct in which the voter is registered.

At the end of the night after the polls have closed and the DRE touch screens are being closed out, the poll workers command each DRE machine to print its "Long Report." The Long Report is of varying length but a constant three inches wide (in rough dimensions). The quality of the paper is similar to a cash register receipt. The print font is smaller than many register receipts. (See Appendix 5 for a Long Report example).

The DRE "Long Report" summarizes in print (on the register-receipt paper) the election results for the ballots that were cast on that particular DRE unit. Each unit's Long Report reflects the internal DRE unit's computer sorting of all ballots and results voted on that DRE unit, providing results by precinct for every race and issue that is present on the ballots that were voted in that location. The Long Report does <u>not</u> reproduce the individual voter's ballot choices; these records are sealed on election night and not opened unless needed for a recount.

In voting locations that are assigned many precincts, the Long Reports can extend well over 20 feet since the results of each precinct must be separately stated on the Long Report. For instance, a voting location with eight precincts but with virtually identical ballots for each

[6] Cuyahoga County uses the Diebold AccuVote TSX with VVPAT printer.

precinct will produce Long Reports that will state the results for U.S. Senate, for Governor, for Attorney General, etc., eight separate times to reflect each precinct's election results. The audit volunteers had to examine closely the Long Report for every DRE unit in a location (which could number as many as 40 units) to locate and record the results for the particular precinct that was randomly selected for the audit.

B. Objectives and Limitations of the Audit

Objectives. The objective of the DRE-GEMS portion of the audit was to determine whether the votes cast in the precincts as represented in the Long Reports are accurately recorded in the CCBOE's GEMS (central computer election tabulation) results report for the *unofficial count*[7] of the election (meaning the election results that were generated on November 8, 2007 not including provisional votes or absentee votes). This audit would thus check to see whether the DRE memory cards' recording of votes that were transferred ("uploaded") into the GEMS computer matched the Long Report results that were printed at the precinct on election night before the memory cards were pulled out and sent to the CCBOE offices[8].

Unexplained discrepancies could mean:

- The voting data on the DRE memory cards became corrupted, lost or altered at some point after the Long Reports were printed from the memory cards at the polls to the point at which the GEMS unofficial report was printed, or

- The GEMS database lost/failed to receive data from the DRE memory cards.

The audit analysis consists of two parts:

(1) A comparison of precinct-level counts between GEMS-produced data provided by the CCBOE (in "csv format") with Long Report data collected by volunteers from a sample of precincts; and,

---

[7] Unofficial results count most but not all ballots. The unofficial results are typically announced late Tuesday night or early Wednesday. In Cuyahoga County, the unofficial count excludes, for instance, provisional ballots, some late arriving absentee ballots, and optical scan ballots cast at the polling places by curbside voters.

[8] It may appear at first blush that the DRE memory cards' arrival in the CCBOE offices for "uploading" is an easy task to achieve. Actually, the process has numerous junctures where an error can lead to an inability to produce complete and prompt election results. A few of the steps are:

- Poll workers must understand the sequencing of closing steps so that they eject the memory cards at the correct time
- All DRE units must be checked to ensure that all memory cards have been collected
- All memory cards in a polling location (which in our county can number high as 40) must be counted and packed into the appropriate bag and sealed.
- The driver/transportation for memory cards must arrive on time and transport the cards quickly to the CCBOE offices

As we have observed locally, the opportunity for mistakes and potential threats to the integrity of the memory cards inhere in the DRE voting system.

(2) An analysis of the "auditability" (ability to be used for an effective audit) of the Long Reports, which concerns their illegibility or unavailability (e.g., due to paper tears, printing jams, or absence from the appropriate envelopes).

Limitations. This DRE-GEMS audit was limited because of (1) Ohio election law and (2) resources. When we obtained authorization for the DRE audit, we presented an ambitious plan for conducting it right after Election Day but before the certified count occurred. This timing was designed so that if any discrepancies were found, they could be investigated and corrected before the legal certified count occurred.[9]

Conducting this audit before the certification meant that the VVPATs of individual voters' ballot choices were off-limits to witnesses and CCBOE staff. State law compelled the VVPATs to remain under seal until the recounts occurred, to protect the integrity of the ballots. (Ohio law explicitly makes the VVPAT record the official ballot and not the electronic ballot when a recount occurs.) Recounts are permitted only after certification. Hence, we could not obtain access to the individual ballots to check whether the Long Reports added the votes correctly.

Even after the optical scanning audit was added to the audit and we knew that we had to wait until after the recounts to conduct that portion of the audit, we did not request to conduct a more exact audit of the DREs' individual ballots to determine whether the Long Reports accurately reported these votes. Our reasons included:

- We knew that we could not produce the number of volunteers necessary for such an audit in mid-late December;
- We believed that we had a significant auditing project already and this was sufficient as a first step in local election auditing;
- We explicitly stated at the time the audit was proposed that it was not the broadest, most optimal election audit that could be run, but we believed it to be a strong initial step toward independent verification of election results;
- Finally, given that the CCBOE Board had planned to initiate a professional audit, any auditing beyond our Collaborative Public Audit effort could be left to the professional auditors.

Our DRE audit also cannot check the accuracy of the GEMS results as compared with individual DRE unit Long Reports. The lowest level of GEMS tabulation results available to us was the results for the precincts – not for individual DRE units. Thus we could not audit a selection of DRE units' reports against the GEMS reported results but could only audit down to the precinct level. This limitation was thus a function of the software design (as represented to us by CCBOE Ballot managers) rather than our auditing policy choice.[10]

[9] Many unanticipated impediments and delays occurred which, with new management and logistical planning at the CCBOE, should not occur in future audits.

[10] Further investigation of whether the GEMS software product has the ability to produce election data by DRE unit should occur; this question was beyond the scope of this audit.

C. Methodology

Overview. Rather than audit 100% of the precincts, audit methodology and statistical science have shown that auditing a random selection of precincts can predict what the error rates would be if all the precincts were audited. The number of precincts to be audited to achieve a 99% confidence level in the predictive capacity of the sample will differ according to the closeness of the results. Closer elections require auditing a higher percentage of precincts.[11]

The Collaborative Audit participants met prior to the election to plan the audit tasks and procedures. Within 48 hours after the unofficial election results reporting, the Audit Committee met to select the races to be auditing. The Committee's selection process resulted in the choice to audit the following three races in the DRE-GEMS audit:[12]

- Ohio Auditor General race between Barbara Sykes and Mary Taylor
- Cuyahoga County judicial race between Hollie Gallagher and Jeff Hastings
- Ohio Supreme Court contest between Terrence O'Donnell and William O'Neill

To ensure that all three races audited in the DRE-GEMS analysis would have a very high level of predictive reliability, the Collaborative Audit Committee (CAC) chose to use the closest race (among those selected for auditing) as the determinant of how many precincts would be audited.

To determine which of these races had been the closest electoral contest, the CAC relied on the unofficial election results reports. These reports included the votes recorded at the polling places on DRE units and also the early absentee optically scanned ballots. If the race was a statewide race, then two results reports were used to determine the electoral margin between the candidates: (a) the state unofficial results and (b) our county's unofficial results. This statistical analysis determined the need for a random sample of 132 precincts to produce a 99 percent confidence level. (See Appendix 1 for complete description of the sampling methodology.)

Dr. Mark Salling and his NODIS team generated a random selection of 132 precincts. The selected precincts were not known to anyone in the CCBOE or in the CAC prior to the audit team's arrival in the CCBOE offices for the audit when Dr. Salling provided the list so that the selected precinct envelopes could be pulled from the sealed bins.[13]

Volunteers and professional staff conducted the DRE-GEMS audit of the Long Reports on November 9 and 14, and December 1, 2006. NODIS professionals created a paper form for audit data to be recorded from the Long Reports. (See Appendix 2 for a sample form). Volunteers were trained on site on where to find the correct data and how to record it on the form. The requested data included:

---

[11] Norden testimony to Elections Subcommittee, see note 3 above,

[12] The CAC selected county or statewide races, with each political party selecting a race and the civic groups selecting the third race.

[13] We recommend that public viewing of the random selection of precincts occur, or that the process be videotaped with the original tape provided as a public record per the Brennan Center report.

- total votes recorded for each candidate in the selected precinct in each of the three electoral contests;
- total ballots cast for the selected precinct;
- DRE serial number;
- audit materials integrity information concerning whether the Long Report was torn, incomplete, or reflected printing problems;
- whether the report was signed at the bottom, as required by Ohio law, by at least four persons (pollworkers); and
- identification of the audit team recording the data.

After the volunteers recorded the Long Report data on the paper forms at the CCBOE offices, copies of these raw data forms were made and held for distribution to each participating organization if requested. The raw data was subsequently entered into a computer at Cleveland State University for further processing and reporting. Center staff then provided copies of the electronic data spreadsheet recording the raw data and copies of the paper raw data forms that were filled out by the volunteers to each participating organization so that they could check the data entry themselves. Special procedures were designed to prevent errors in volunteers' data collection, to verify the data in an ongoing manner, and to provide a traceable path that could be checked and permit correction of errors in case any were discovered.

Detail of Chain of Custody and On-site Audit Activities. The first on-site step in the audit process was locating the envelopes for the selected precincts. The Long Reports, as mentioned above, are long cashier tape paper rolls printed from each DRE within a given voting location. On Election Day evening, as the polling place materials arrived in the administrative offices for tabulating the vote, CCBOE staff removed (in front of trained witnesses) the extraneous materials from Long Envelopes (that had been sealed at the polling places) and then replaced the Long Reports in the correct precinct envelope with a new seal.[14] The staff then placed all the Long Envelopes (that were labeled with a polling location name and that had been stuffed with the Long Reports) into bins that were sealed with recorded seal numbers. The staff did not file the Long Envelopes in any particular order, thus the volunteer auditors had to check each bin seal to ensure the unbroken chain of custody. They then searched through approximately 40 large bins to find the polling place Long Envelopes that would contain the randomly selected precincts' Long Reports.

Working in teams of two and seated at tables in the same room where the polling place materials had been processed on Election Day, the volunteers examined each Long Report from a given polling place to locate the precinct results for the three races to be audited. Because voters from all precincts assigned to the location could use any DRE within their polling place, every DRE Long Report used in a particular polling place had to be examined for whether any of the chosen precinct's voters had cast ballots on that machine. Unrolling and re-rolling the narrow and relatively fragile Long Reports (which could easily stretch over

[14] Midway through the night, the CCBOE staff ceased resealing the envelopes because of time pressures and chose to rely on the storage bins being sealed.

20 feet long) was a very time-consuming and tedious process.[15] Selected precincts that were located in a polling place having few DRE units were much quicker to audit since fewer Long Reports had to be analyzed.

For each precinct analyzed, the volunteers took an audit data form and recorded at the top their names, the time they started, and the time they finished. For each Long Report, they recorded the DRE serial number printed at the top of the Long Report, the total number of ballots cast from that precinct, and the number of votes recorded for each candidate in the three audited races. They also noted and recorded information and characteristics about the report (e.g. if it was torn and how many poll workers signed at the bottom). The name of the polling place stated on the Long Report was always verified.

By working in pairs, each data step was double-checked by at least one person. One person read the results off the Long Reports while the other recorded the data. Periodically, they were then required to confirm each other's work.

Evaluating the Audit Data The data that volunteers recorded at the CCBOE was entered into a computer. Then this Long Report data was compared by precinct to GEMS-produced data (on electronic files), with careful notes as to which results did not match in all races and total votes cast. Professional staff looked for and corrected any computer data entry errors that resulted in any of the unmatched results and then examined the data recording sheets for factors that would account for unmatched counts. When there were discrepancies that could not be explained, volunteers returned to the CCBOE to pull the appropriate Long Reports and double check their auditing work. By following this approach, we were able to ensure that no discrepancies occurred because of auditor data-recording errors.

The Center's professional staff also calculated the frequency of discrepancies that occurred as well as all Long Report materials problems (e.g., torn, incomplete, or unsigned).

D. Findings

Comparison of Counts and Accuracy of the Tabulation. Among the 132 precincts for which we recorded Long Reports data, 95 precincts' election results data for the three races and total ballots cast perfectly matched the GEMS computer data for all three races and total ballots cast. While it is possible that the Long Reports data match the GEMS data only because of balancing errors in both, the probability of that occurring is extremely small. Thus we conclude that since the data in the DRE Long Reports correctly matched the GEMS counts for those precincts and within the limitations discussed above, both sources of data correctly presented the votes for those precincts and election races.

Among the remaining 37 precincts (see Appendix 6 "All Unmatched Precincts"), for some precincts the data collection was harmed owing to torn or illegible Long Reports that affected only a portion of the three races to be audited. Wherever we had a complete set of results for a chosen race, we compared those races even if one or both of the other races' data could not

[15] By chance, the largest polling location in Cuyahoga County, Brook Park -- having 40 DRE units – was in our random sample. So we had to analyze all 40 Long Reports in order to record the one selected precinct's data.

be analyzed because the Long Report was torn or quit printing in precisely the location where that needed data was located. We found that Long Reports from six more precincts had sufficient data that at least some of the three races were auditable. For each race that could be audited, the Long Report data matched the GEMS computer data exactly.

The other 31 precincts, however, were not auditable because, owing to one or more materials problems with the Long Reports (including missing reports, reports that were torn, reports reflecting printing problems due to printer jams), some essential data was not available for each of the three races we were auditing. The Long Reports deficiencies for these 31 precincts were noted by volunteers when they were attempting to record all the requisite election data needed.

Missing or defective Long Reports led to an inability to audit a sample size as large as originally planned. The sample design attempted to take into account a limited number of such problems by adding another 20 percent to the sample size. Clearly the problems of missing or damaged reports exceeded reasonable expectations.

Points Raising Concerns

Duplicate DRE Serial Numbers. We found several Long Reports with the same DRE serial number but that recorded different election results (see Appendices 4 and 5).

In one case, two sets of two DRE Long Reports (each pair having the same DRE serial number) presented different vote counts. Rather surprisingly, each of these two pairs of DRE machines was assigned to a common polling location. In each of these cases, the votes reflected in each of the four Long Reports appear to have been included within the GEMS totals; when we included all four DREs' votes for comparison with GEMS, the GEMS totals matched the Long Reports perfectly.

In another case of duplicate Long Reports, we found a pair of reports from DRE units having the same DRE serial number, but these DREs were assigned to different polling locations.

When asked about these duplicate serial numbers, a representative of the CCBOE stated the following in an email:

> It appears as though Diebold transposed serial numbers when it loaded firmware [vendor-installed operating software] into these machines. The serial numbers on the machines themselves are sequential (hardware). This is problematic because the linkage to the memory card is off the serial number presented by the screen....

If indeed the serial numbers were entered by Diebold, including some mistaken duplicate numbers, and then shipped to the CCBOE, the chances of two machines with duplicate serial numbers ending up at the same polling location within our sample is extremely unlikely. Given that we found this situation twice in our sample, this explanation merits further exploration. We have not been provided any further explanation from Diebold or from the CCBOE.

No DRE Serial Number. The audit found 19 instances where the DRE serial number was missing from the Long Report or otherwise unavailable. This problem relates to the issue of torn and printing problems noted above.

Five-digit DRE Serial Numbers. Of unknown implication and importance we note here that we found two instances where the recorded DRE serial numbers were five digits in length. This is at variance from the six-digit length that we found for all the other serial numbers that were recorded. While this might be a data entry error in the audit process, it also may reflect an error in the manufacturer's creation of the serial numbers. We did not make an extra check to ascertain whether it arose from a data entry error.

Other Problems with the Long Reports

Legally Required Poll Worker Signatures: Among the 1,168 DRE Long Reports that the auditing teams examined, 354 or 30 percent lacked the legally specified four signatures. Among these 181 (16 percent of the total) had three signatures, 63 had only two signatures and two Long Reports had only one. 108 Long Reports weren't signed at all (9%).

Defective Long Reports: Volunteers recorded information showing that 95 reports (8%) were torn, incomplete, or had apparently jammed in printing and that they either lost or may have lost Long Report data that was to be printed. These figures exclude instances where we found a second Long Report from the same DRE unit, evidently printed to replace a report with such problems. Given that we found and used for the audit a number of what appear to be replacement Long Reports, the 8% figure for the rate of defective Long Reports is a lower rate than actually occurred.

Lack of Agreement between Unofficial PDF Versus Sum of Three CSV Files. The PDF file of unofficial results that the CCBOE posted on its website presents totals that differ by very small amounts from the sum of the three unofficial CSV files (DRE polling place, early absentee on optical scan ballots, and "walk-in" absentee ballots on DREs at the CCBOE) we obtained from the Ballot Department to use in our audit.

The accumulation of vote totals in the CSV files and the election results as presented in the published PDF file should reflect the exact same totals for the unofficial results, but 128 precincts out of the 1,434 in the county do not match. They generally only differ by one or two votes. We do not have an explanation for this discrepancy (see Appendix 7 for complete list of precinct discrepancies). For fuller exploration of data reliability issues, see Section IV.

E. Conclusions

Conclusion 1

There is a high probability that the DRE Long Report results match the GEMS produced data for the election on November 7, 2006.

This conclusion is important and reassuring. For all of the randomly selected precincts for which the Long Reports were legible and available, the Long Reports vote totals for candidates matched the GEMS election results exactly. More precisely, of the 132 precincts randomly selected for the audit, 95 matched the GEMS totals exactly. The balance of the precincts could not be evaluated because of missing or incomplete Long Reports.[16]

Conclusion 1, however, assumes that the Long Reports accurately reflect the ballots cast. As explained above in the report, the accuracy of the Long Reports was not evaluated by this audit. To be clear, for an election audit to be able to assess the likelihood that voters' ballots cast on DRE units are accurately reflected in the reported election results, we would need audits (using scientific sampling) of at least three separate phases of the election vote-recording and tabulation process:

a. an audit of the individual voters' ballots cast on DRE units to determine if the Long Report (a summary of all ballots and votes cast on that unit) accurately reflected the votes; *plus*

b. an audit checking the correspondence of the DRE Long Reports to the GEMS tabulation data; *plus,*

c. an audit of the GEMS tabulation data to determine whether the results reported in the Totals lines accurately reflect the votes in the selected columns.

Additionally, for utmost confidence in reported election results, an audit covering all three phases is needed at both the pre-certification and after the official canvass or certified count stages of election reporting.

Conclusion 2

Expecting a complete set of DRE Long Reports with all data clearly recorded for all precincts currently is *not* realistic.

This conclusion is based on the problems we encountered with Long Reports (e.g., torn, missing, printing problems) in 37 of the 132 precincts in our sample. The 132 precincts within the sample included 1,414 DRE machines so that would mean that 1,414 Long Reports were analyzed. Of this number, 181 (13%) were not auditable. Since, as noted above, voters could lawfully vote on any DRE in the polling place, some of these Long

[16] We determined whether there were "missing" Long Reports based upon an electronic file we received from the CCBOE listing the number of DREs at each polling place. We expected to find a Long Report for each DRE. It should be noted, however, that the CCBOE apparently had another list with a slightly different DRE count per polling place. As we had no way of knowing which was more accurate, we used the file sent to us via official CCBOE channels.

Reports recorded results for more than one precinct in our sample. In those cases, the damaged Long Report could cause the exclusion of two randomly selected precincts from the audit.

These results are consistent with the ESI report's finding that 9.66 percent of the VVPAT ballots were defective or compromised in some fashion in the May 2006 primary.[17]

Some of the Long Reports that CCBOE workers could not find for us may exist but could have been misfiled within the CCBOE on Election Night because precinct materials were flooding into the building and the staff was focused on retaining and uploading memory cards.

Producing legible and complete Long Reports is difficult for a number of reasons:

- Printer jams are common;
- With the addition of electronic voting and voter ID requirements, poll worker duties have become more complicated;
- Changing and reloading TSx printer paper is a complicated process, with a number of possible errors that can cause printer failure or marred Long Reports
- In this county, nearly 6,000 Long Reports will need to be produced by poll workers who have had four to eight hours of training (often occurring weeks before the election); and
- At the closing of the polls when the Long Reports need to be printed, poll workers are tired and the focus is on hurrying to obtain the memory cards so they can be sent for tabulation.

Neither this recommendation nor its attempt to outline the causes of defective Long Reports should be taken to suggest that the CCBOE should relax or eliminate the effort to achieve proper printing of the Long Reports at the polling places. Improvements in poll worker training should help to reduce the number of problematic Long Reports, and this should be an objective when planning improvements for poll worker training.

Yet we must also point out that a voting system that leaves 8-13% of the precincts unauditable is highly problematic and will likely have serious consequences for voter confidence.

Conclusion 3

Some DREs have serial numbers that are non-unique and duplicate those found on other DRE units owned by the CCBOE.

Our audit discovered some Long Reports having duplicate serial numbers, apparently printed by separate DREs that have been manufacturer-marked with the same serial number. Given that we found this problem in a random sample of Long Reports having predictive capacity, it is likely that other Cuyahoga County DREs have duplicate serial numbers. The Board of Elections believes that this duplication occurred due to Diebold transposing serial numbers

[17] "DRE Analysis for May 2006 Primary Cuyahoga County, Ohio," Election Science Institute (August 2006), 102-124.

when it loaded firmware into the DREs, thus resulting in two machines having the same serial number.

Duplicate serial numbers raise at least three *potentially* harmful outcomes for the accuracy of vote counts, dependent upon whether certain safeguards are embedded in the GEMS software; this professional assessment of GEMS protections is beyond the scope of the audit. First, if GEMS is allowing data associated with the same serial number to be uploaded twice, votes from the same DRE could potentially be counted twice. Conversely, if two DREs have the same serial numbers, there is a risk of GEMS not allowing the votes from both voting units to be uploaded and overwriting the votes of one machine, thus losing votes. Third, correct and unique serial numbers are also essential for being able to pull the correct vote records from DRE flash memory when a memory card is missing or unusable.

Additionally, at least three *possible* logistical and administrative problems are raised by the duplicate serial number problem. First, duplicate serial numbers make it impossible to audit machine performance across multiple elections. Second, the serial numbers may also need to be unique for warranty purposes. Third and last, the duplicate numbers may impede correct internal tracking of the machine's physical location in CCBOE records.

F. Recommendations for CCBOE Action

Recommendation 1

Develop an Independent Random Audit Policy and Practice for Validating E-Voting Election Results.

We recommend that an independent random audit of the election results be performed before CCBOE certification of the election. Ideally, however, to verify the official count and its reported results, an audit would be performed after the official count but before those results were presented to the CCBOE Board for a certification vote. This timing would be optimal, because it is the point at which all ballots have been counted and the CCBOE believes it is ready to certify the results. Thus, any discrepancies can be corrected before certification. Given, however, that the Ohio General Assembly recently shortened the time frame for certification by almost a week, this optimal timing of the audit may not be feasible. But with advance logistical planning and better procedures and staffing within the CCBOE, it might still be possible to achieve this objective.

The largest problem currently, however, is the lack of any CCBOE procedures to undertake an independent verification of the election results generated by the GEMS software results before certification. Quoting the Brennan Center landmark report "*The Machinery of Democracy: Voting System Security, Accessibility, Usability, and Cost*:"

> Systems with voter-verified paper records provide little, if any, security benefit over systems without such records, unless there are regular audits and/or recounts of the paper records.[18]

The Collaborative Audit Committee is willing to work with the CCBOE to develop a plan and procedures under which expedited random auditing of every election and to help identify the time frame within which the auditing can occur. This Audit Report can provide a template of the explanatory information the public needs to understand the process. Overview material about the voting systems can be simply restated with each election audit so that the audit report could be issued very quickly.

While undoubtedly the best source for verification of the results is to use the voter-verified paper audit trail (VVPAT), by State law the VVPAT cannot be unsealed until the recounts occur (after certification). Statutory law further bars auditing activities that might piggyback on the recount process. Given these state law impediments to random auditing of the VVPAT before certification and also during the recounts, it may be that auditing the Long Reports as against the GEMS results is acceptable until state law changes can be achieved.

Because eight to ten percent of the Long Reports are likely to be damaged and unusable in verification procedures, their value for verification audits is compromised. But it appears that use of the Long Reports is the only mechanism for auditing DRE units at present. Thus, neither this recommendation nor its attempt to outline the causes of defective Long Reports should be taken to suggest that the CCBOE should relax or eliminate the effort to achieve proper printing of the Long Reports at the polling places so long as the DREs are being used. Improvements in poll worker training should help to reduce the number of problematic Long Reports, and this should be an objective when planning improvements for poll worker training.

Yet we must also point out that a voting system that leaves 8-13% of the precincts unauditable cannot command the voters' trust. This high proportion of unauditable precincts means that in many races, the margin of victory is substantially closer. We understand that the vendor is planning to introduce a new printer model that may have fewer problems. But we believe (given the issues identified in bullet points immediately above) that the human elements and the fact that virtually no mechanical device is 100 percent perfect will mean that the printers will continue to produce a proportion of problematic VVPATS and Long Reports.

These facts about the rates of precinct unauditability owing to printer difficulties should be taken into account when assessing the long-term viability of using the DREs in Cuyahoga County.

[18] "The Machinery of Democracy: Protecting Elections in an Electronic World," Brennan Center Task Force on Voting System Security, Brennan Center for Justice at NYU School of Law, 2006.

Recommendation 2

As part of the planned security review, the CCBOE should assess the viability of using Long Reports as part of its overall security and accountability plan.

Our audit calls into question the feasibility of expecting to use Long Reports as part of any oversight or audit process because of the frequent problems encountered in printing them. The technology and human factors involved in producing the Long Reports should be evaluated to determine if the process can be improved or replaced by other security methods.

Recommendation 3

Resolve the non-unique DRE serial number problem by taking a number of actions.

The occurrence of duplicate DRE serial numbers raises the possibility that the vote totals from one DRE unit may overwrite votes from another unit or be counted twice. Duplicate DRE serial numbers may also lead to CCBOE inability to identify correctly a DRE unit whose internal (flash) memory needs to be used for the re-creation of voting results (normally when a memory card is missing or damaged), and other problems discussed above. These potential problems present sufficient cause to warrant further investigation by qualified independent professionals (not manufacturer employees or contractors) and a public report on findings and corrective actions taken.

We believe the following steps are needed:

- Determine all the purposes for which DRE serial numbers are used within the CCBOE;
- Investigate the extent of the problem of duplicate serial numbers on DREs by checking both the number located on the external casing of every DRE unit and also the serial number that has been loaded into the firmware and publish the results of the inquiry;
- Fully investigate and analyze why duplicate serial numbers were found on Long Reports and what the consequences are for vote tabulation (e.g., whether votes can be uploaded twice or overwritten because of this problem);
- Require the vendor (Diebold Election Systems, Inc.) to correct the non-unique serial number problem and also pay for the investigation of the extent of the problem; and
- Create and maintain a database of all DREs to track serial numbers, testing results, polling place location, malfunctions and service history, lifetime vote totals, and warranty information.

III. Optical Scanning: Audit of "Early Absentee Ballots"

A. Background

"Optical scan ballots" are paper ballots that list each race or issue and provide ovals beside each voting choice. The voter is directed to color in the oval beside the candidate or issue answer that reflects the voter's choice. Cuyahoga County's optical scan ballots are printed on both sides. The optical scanner is a device that reads and records the ballot choices the

voter made if his/her marks were made correctly. Underlining a candidate's name or placing an X in the oval, for instance, are not valid marks that the scanner can read.

While some election jurisdictions use scanners at the polling place to scan ballots and tabulate voting results for each precinct (a "precinct-count" system), Cuyahoga County and other jurisdictions scan all optical scan ballots at a central location (a "central-count" system). Numerous scanners are used simultaneously to scan the ballots. Scanners are linked together in a network with the GEMS computer, which receives and records the scanned voting data and tabulates the election results.

In Cuyahoga County, optical scan ballots are provided to a number of different types of voters. All mailed absentee ballots are paper optical scan ballots, whether mailed to homes in Cuyahoga County or to overseas absentee voters. But paper optical scan ballots are also provided at the polling places for provisional ballot voters and for "curbside" voters who are disabled and cannot enter the polling place to vote. Additionally, backup paper ballots are provided to each precinct in case there were problems with the DRE touch screen units or excessive wait times for voters.

in November 2006, Cuyahoga County's policy was to scan, tabulate, and announce in its "unofficial results" only those absentee ballots that were received in the CCBOE offices by Friday, November 3rd, at 5:00 p.m. These are often called "***early absentee ballots***." As these voted ballots arrived during the weeks preceding Election Day, the CCBOE staff sorted the absentee ballots (still in their sealed envelopes) into precincts. Then, beginning on Saturday, November 4th, CCBOE staff opened, unfolded, and stacked the paper ballots so that they could be compressed flat. This flattening process was designed so that the ballots would be more easily fed into the scanners and the scanners would be more likely to read the votes correctly.

All absentee ballots that arrived after the Friday cut-off time and all precinct-cast optical scan ballots were segregated from the early absentee ballots and locked up until after Election Day and the unofficial results were reported. These later-arriving absentee and precinct-cast paper ballots were counted and presented only as part of the ***official, certified*** election result totals.

B. Objectives and Limitations of the Audit

Objectives. The objective of this portion of the audit was to ascertain whether the early absentee ballot votes were accurately reflected in the GEMS reports of the unofficial electoral results. A hand count of randomly selected precincts' early absentee ballots by teams of volunteers was compared with the GEMS totals to check for any discrepancies. Unexplained discrepancies could indicate any of a number of different types of problems. Unlike the DRE audit, which only audited summary data by precinct from Long Reports, this audit of optical scan ballots compared actual voted ballots with the GEMs tabulation.

Limitations. As with the DRE audit, this audit of early absentee ballot scanning was of a limited nature because of (1) Ohio election law and (2) resources. When the major political parties requested the extension of the collaborative audit to encompass optical scan absentee ballots, we checked with the CCBOE on when the audit's necessary hand count could occur.

The Ballot Department managers said that, as with the VVPAT, the paper ballots would need to be locked, sealed, and unavailable for auditing until after certification and all recounts, per the Ohio recount statute. This meant that the absentee ballot hand count could not occur until mid- to late-December.

Conducting this scanning audit after certification and the recounts meant that we were in the midst of the university exam and December holiday season. We knew that it would be difficult to assemble sufficient volunteers to conduct a hand count of three races so the CAC chose to audit only one race, that of the State Auditor (Sykes-Taylor). We also knew that since the CCBOE Board had announced a plan to undertake a professional audit, any optical scan auditing beyond our Collaborative Public Audit effort could be left to the professional auditors.

Given that we only hand-counted one race and compared these results to the GEMS totals produced in the unofficial count, the audit conclusions are limited. We know that sometimes, depending on the ballot location of a race and how close its placement is to the vertical column lines, the scanners may prove differentially accurate in reading votes.[19] Our audit of only one race could not take account of such factors and identify resulting discrepancies. The Logic and Accuracy testing of the scanners is supposed to identify any problematic scanners so that the CCBOE deploys only those scanners having a perfect accuracy in reading paper ballots are used.

C. Methodology

Overview. At the request of the Audit Committee, Dr. Mark Salling and Ellen Cyran of NODIS at CSU generated a random selection of precincts different from that used for the DRE audit. The 72 precincts selected provided a 99% confidence standard. The Audit Committee selected the State Auditor's race for the Audit.

Detail of Chain of Custody and On-site Audit Activities As noted above, the CCBOE staff sorted the absentee ballots (sealed in their envelopes) into precincts. They were then taken to locked rooms to be preserved until time for opening and scanning. On Saturday, November 4, the early absentee ballots were removed from the locked rooms and brought to the "pink room" for opening. The ballots were placed flat in stacked bins. The bins were placed in locked rooms until the time for the early scanning. The CCBOE staff then sorted the ballots into pre-marked envelopes so that each precinct's ballots could become a "deck" unless the precinct had a particularly large number of ballots cast. Then the precinct's ballots were divided into two or three separate decks. The CCBOE purchased a machine that counted the number of ballots that were in each envelope, and staff recorded the number on the envelope's label.

[19] *See, e.g.*, the CERP Final Report concerning the scanning problem in May 2006, in which only particular races were not read accurately and correlated highly to ballot placement and formatting issues. Also see the Systest Labs Report concerning the optical scanning problem that is found in CERP Appendix.

The early absentee ballot envelopes were brought down to the basement scanning area that had been specially constructed for this early absentee scanning. Up to 100,000 absentee ballots were expected to have arrived in time for the early count—many times more than in any previous election.[20] After the early absentee scanning on November 6, the ballots were locked again.

The on-site hand count audit activities occurred on December 6, 8 and 29, 2006. A team of volunteers returned on February 16, 2007 to double-check discrepancies. At the outset of each day of the audit, approximately 20-30 precinct files (the number the auditors felt they could complete in the day) were pulled by CCBOE staff from the third floor vault where all early absentee ballots were stored. Members of the audit team observed the unlocking of the ballot vault and the transporting of the optical scan ballots to the "pink room." At no time during the audit activities did the auditors leave the ballots unattended or unsecured.

The CCBOE managers represented that even though the audit occurred after all recounts, only CCBOE staff could legally touch the ballots.[21] This rule meant that scheduling the hand count of the optical scan ballots was dependent upon the availability of CCBOE staff.

Each hand count team of auditing volunteers was composed of four people: one "reader" of the ballot/race, one "observer/confirmer" that the reading was correct, and two "recorders" who recorded separately.[22] Because only CCBOE staff can touch a ballot, one CCBOE staffer handled and turned each ballot as the vote was being read and recorded by volunteers. The CCBOE assigned two of their staffers (one Democrat, one Republican) to be present at all time per the managers' representation of the law governing the handling of voted ballots.

The audit recorders first recorded in ink on the audit forms (see Appendix 8 for sample form) all location and batch information from the label on the front of the precinct envelope. The CCBOE staff (with close monitoring by the four auditor volunteers) then separated out the pages that contained the State Auditor race. This segregation of the needed ballot pages generated a faster auditing process. Upon realizing that some decks included some ballots from other precincts mixed within the selected precinct ("misfilings"), the reader and confirmer (and CCBOE staffer) checked the name and number of the precinct on the bottom of each page to make sure it was from the correct precinct.

All votes were to be classified in one of four ways by the reader who called out the vote: "Taylor" or "Sykes" or "no vote" or "unable to determine." The confirming volunteer watched carefully to ensure the accuracy of the reader's call. Periodically volunteers switched roles to keep everyone fresh.

---

[20] Reasons for the sharp increase in absentee ballots included (1) the 2006 Ohio statutory change to permit "no-excuse absentee ballots" (allowing virtually any voter who wanted to vote by absentee to do so), and (2) the Cuyahoga County Commissioners' public campaign to encourage voting by absentee ballot.

[21] We are not sure that this representation as to the legal constraints on touching the ballots is correct. In the summer 2006 ESI audit of the VVPAT, it appeared that ESI employees were touching the DRE ballot as a part of their audit activities.

[22] State law hand count "best practices" collected in the study that the U.S. Election Assistance Commission funded provide for at least these four positions in a hand count team to ensure accuracy. (Study by Prof. Thad Hall of the University of Utah is not yet available via the EAC website.)

Two volunteers independently recorded the vote on the audit reporting form. They ensured that every ballot page on which the selected race was presented was reflected by a record in one of the four categories listed on the audit report form. After approximately every 20 ballot pages, the recording process paused so the two recorders could compare their tallies. By proceeding in this manner, if tallies did not match, the team only had to review the last 20 ballots to find the recording discrepancy rather than a full deck of ballots. Once all the votes in the race were recorded for all ballots for the precinct, the recorders independently tallied the results on each form. They then placed the results at the bottom of the form and compared them to each other to ensure that the grand total for each candidate in that precinct matched across the sheets.

This hand count data was later entered into a CSU computer database and then the computer data was checked for data entry mistakes. The hand count results were then compared to electronic files provided by the CCBOE.[23] These files are discussed in more detail below.

D. Findings

We were able to audit (via our procedures for hand counting) all 72 precincts in our random sample of early absentee ballots. The ballots from two of the precincts (Cleveland 13-O and 17-K) could not be located during our first round of audits (December 6 – 8, but Ballot Department employees were able to track them down for our follow-up visit on December 29. Upon investigation, it turned out that these missing ballots had not been filed in the correct envelopes but by looking at batch numbers, the Ballot Department was able to figure out with which precinct they had been scanned and accidentally misfiled. This misfiling would not have affected the GEMS tally because each ballot page is computer-coded with the precinct's identifier.

After the original on-site audit activities and the first follow-up, a comparison of the hand count audit data with the GEMS tabulation report showed the hand count results were consistent with the GEMS precinct counts for 43 of the 79 precincts. Most of the 29 tallies inconsistent with the GEMS report differed by only plus or minus one vote. One precinct showed one more vote for Taylor and one less for Sykes than the GEMS report. One precinct, however, contained 60 ballots in its folder while the GEMS report showed zero ballots had been tabulated for that precinct. These differences are documented in four groups in Appendix 9.

Discrepancy Evaluation: Off by One or Two Votes Possible explanations or causes of the discrepancies of a few ballots include (1) errors in counting by audit volunteers during the hand count; and (2) incomplete or inaccurate sorting of ballots prior to scanning resulting in ballots from another precinct being present in the folder that was audited and/or ballots from the audited precinct being misfiled in a different precinct folder.

> *Regarding Possible Explanation 1*
> During the original audit, each team had two observers who examined the ballot pages before calling out the voter's choice, and their observations were independently recorded by two other volunteers who then reconciled their results at several interim steps as

[23] For the purpose of the optical scan audit a file labeled *"GEMS SOVC REPORT Unofficial AVOS Only.pdf"* was used based on guidance from the Ballot Department managers (see Appendix 13 and Part IV of this Audit Report).

described in the procedure section above. Additionally, at a subsequent return visit to the CCBOE, 11 of these 29 discrepant precincts were re-counted. No errors in the hand count were detected.

Regarding Possible Explanation 2
The central count tabulation report for the unofficial count was made available by the Ballot Department. This report shows each group or "batch" of optical scan ballots and shows the number of ballot "cards" (pages) in each batch and to which precinct each ballot "card" was assigned. Close examination of this report showed that the ballot pages of 307 precincts were filed in more than one batch, and that 201 batches contained ballot pages from more than only one precinct. It was also noted that in the Central Count Report, 12 precincts showed no ballots had been counted and no votes had been recorded.

Auditors returned to examine these discrepancies on February 16 (see Appendix 10 for complete description). Eleven of the precincts with fewer ballots in the hand count than reported by GEMS were found to have misfiled ballot pages, scanned in with a different precinct. Five of the precincts with fewer hand counted ballots could not be explained by misfiling. Of the 11 precincts in our sample with a higher hand-count than the GEMS report, three were found to be filing errors in which another precinct's ballots were included in the wrong precinct deck and the auditors mistakenly included them in their hand count.

The remaining eight discrepancies could not be explained by filing or hand-count errors. The hand count for the precinct with one higher vote and one lower vote for the two candidates was rechecked and found to be accurate. No explanation for the discrepancy with the GEMS report could be found for this precinct.

Discrepancy Evaluation: Precincts with No Votes Recorded in the GEMS Report
The finding of greatest concern was the precinct, North Olmsted 2-F, which was found to have ballots in the precinct folder but no results reflected in the GEMS election results. This precinct was also one of the 12 that did not show any ballots counted in the Central Count Scanning Report. Auditors returned to examine all 12 of these precincts (expanding beyond the original sample) to see how common this problem was.

The CCBOE apparently received no early absentee ballots for eight of these 12 precincts that recorded no ballots counted. Four precincts were found, however, where it appears likely that all or nearly all of their early absentee ballots were not included in the unofficial SOVC Report[24] (see Appendix 11 for a complete description).

Auditors were able to physically examine the ballots and envelopes of three of these four precincts where the GEMS election results showed no early absentee ballots had been tallied. In our view, it appears that these precincts' ballots were scanned but then deleted from the GEMS tally (see Appendix 12 for the CCBOE's explanation of the omission). The precinct folders the auditors examined contained ballots in numbers corresponding to the number of

[24] The SOVC Report is the comprehensive Statement of Votes Cast Report from GEMS. It can show, precinct by precinct, the total votes cast for every candidate and ballot issue and thus is quite lengthy unless a selected portion is requested for printing.

early absentee ballots that the CCBOE staff in the Candidate and Voter Services Department had recorded as returned in time for early scanning.

The CCBOE procedure during the early scanning for the unofficial count required verification by the ballot tabulation staff that the number of ballot pages GEMS reported as having been scanned was within a certain margin of error of the number of pages reported by the scanner. If not within that predetermined margin of error, the tabulation staff was supposed to delete the precinct batch result from the GEMS tabulation. They were then to send word to the scanning room with 60 teams of scanning personnel that the deleted deck was to be rescanned. In these cases, it is possible that after deleting the precinct batch from GEMS, the ballots were not rescanned but simply refiled in the envelope. Two precincts each showed one vote in GEMS because there was a single ballot card for each of those precincts present in a deck that consisted of only the single card.

Discrepancy Evaluation: Ballot Decks Scanned Multiple Times While comparing the SOVC electronic file with the reported numbers of absentee ballots returned, it was also noted that for at least two precincts (not originally included in our sample) it appeared that there were significantly more votes recorded than were absentee ballots. Specifically:

North Royalton 3C	*770 voters*	*52 abs returned*	*118 SOVC*
Euclid -02-J	*896 voters*	*73 abs returned*	*142 SOVC*

Examination of the Central Count GEMS report for these precincts shows each to have had 2 batches of identical or near identical size with sequential or near-sequential numbers. When we examined these precincts' folders, there were ballots present in the folders in numbers consistent with the number of absentee ballots reported returned. These observations are all consistent with an explanation that the ballots in these two precincts' folder were scanned twice and that the votes on each ballot had been included in the SOVC election results twice.

E. Conclusions

From the limited scope of this audit, which examined the results of one race as recorded on early absentee optical scan ballots that were part of the unofficial count, we may conclude the following:

Conclusion 1

Election result data in the GEMS report corresponded closely to the results obtained by the audit hand count of the optical scan ballots

Audit results either matched exactly or were discrepant in a manner and degree consistent with the number of ballot pages misfiled for 57 of the 72 precincts included in the audit. Fourteen of the 15 precincts that did not exactly match were discrepant by plus or minus one vote with an aggregate of one more vote for Sykes and three more for Taylor found by the audit. This is a low net error rate out of a total of 3628 votes. The one other discrepant precinct was not reported in the unofficial SOVC at all and represents an apparent scanning procedural error.

Conclusion 2

The sorting process for early absentee optical scan ballots into precinct batches prior to scanning was neither complete nor accurate.

A total of 1,768 "decks"[25] were created in which the early absentee ballots from the 1,434 precincts in Cuyahoga County were placed. Of these 1,768 decks, 201 contained ballots from more than one precinct. The election reports also show some ballot pages of 307 precincts were separated (possibly misfiled) into more than one folder.

Prior to commencing the scanning of the early absentee ballots, the CCBOE staff hand sorted a total of 66,228 absentee ballots into precinct decks. We were able to identify patterns of misfiling: often the ballots were misfiled into precincts where extremely similar precincts codes to the correct code were used. These codes often differed by only one character. This pre-sorting was necessitated by concerns about the GEMS database's limitations and its stability over the period of uploading optically scanned ballots. Although the sorting was imperfect, without it we would not have been able to conduct this audit and compression of the GEMS database—and its consequent risks -- would have had to occur much more often.

Conclusion 3

Some discrepancies that occur at a very low frequency appear to be caused by a scanner misreading of some of the optical scan ballots.

[25] A "deck" is the electronic representation of a batch of ballots that were to be scanned together. The scanner sends the accumulated results of the ballot up to the GEMS computer as one deck tally. This deck approach is in lieu of scanning 55 ballots separately and sending 55 separate vote tallies up to GEMS. By using sizable decks, the GEMS database does not grow as fast as having more decks with fewer ballots in each.

In several of the discrepant precincts, the correct number of ballots was identified in the initial audit and in a subsequent follow-up visit. However, the GEMS reported results differed in a pattern suggesting that one or more ballots that the auditors considered to have been clearly marked in either blue or black ink had not been accurately read or recorded by the scanners/GEMS. In these cases, one fewer vote would be reported in the GEMS data file.

Conclusion 4

Some ballots were apparently scanned at some point but were not included in the GEMS results or on the SOVC election results report.

At least four precincts for which early absentee ballots had been returned showed no votes recorded in the unofficial election result tabulations. In at least three cases, it appeared from the ballot folder documentation that ballots had been scanned and must have been deleted but not rescanned.

Conclusion 5

Some ballot batches were scanned twice with their votes double-counted when the GEMS unofficial results and the SOVC election results report is analyzed.

The ballots in at least two precinct folders appear to have been scanned twice. The numbers of optical scan ballots present in the folder was consistent with the number of absentees returned while the results reported in the election result tabulation for these precincts were approximately doubled.

Conclusion 6

Batch/deck numbers identifying specific groups of ballots may change within the scanning process and between scanning events.

The deck/batch identification is arbitrarily assigned by the "header card" that is placed at the front of a stack of optical scan ballots prior to their being scanned. As reflected above, a batch can be rescanned with a different header card. Similarly, some of these ballot batches were given different digital batch identities when they were re-scanned for the official count. The change in ballot batch identifiers greatly impeded the accurate tracking of batches so that they could be confirmed as having been counted, and counted only once in the election tabulation.

F. Recommendations for CCBOE Action

Recommendation 1

Hand sorting into precinct batches should be replaced by an automated system.

If the CCBOE has a continuing need to sort received absentee ballots into precinct-based groups, this process should be automated. All of the absentee ballots originate with the

CCBOE and are machine addressed. Automated sorting of the returned ballots could be done by a commercial mail handler using a barcode placed by the CCBOE at the time of addressing the mail to the voter.

Recommendation 2

The labeling or identity of a batch (and its electronic representation as a "deck") should be unique and constant.

Each deck of ballots should have a unique and immutable identity code, and ballots should not float between decks. If the CCBOE continues to sort by precinct, this could be a precinct-based code. Such a system would enable tracking and accounting for all ballots received. It would also facilitate an audit of the performance of the optical scanning system.

Recommendation 3

A mechanism should be developed to record and track specific batches of ballots.

Each uniquely identified deck of ballots should be scanned and included in the election results one time and only one time. Possible approaches to such a system include a precinct-based system that counts and reports the number of absentee ballots received by the CCBOE as the precinct bar code is read on the intake sort. A system that uniquely identifies ballot decks, prevents the double counting of ballot decks, and has the ability to flag missing decks would be a major improvement over the uncontrolled situation that now exists.

Recommendation 4

The process of deleting ballot batches must have greater quality control to ensure re-scanning of the deck.

Deletion of ballot batches means a large number of ballots are not recorded in the tabulation unless rescanned. The CCBOE did not use the paper and ink log to record events such as this, and there was deficient quality control and procedural verification over whether deleted batches were re-scanned. Improving the quality control over the scanning procedure is the best solution. However, an easy *interim* step is to perform a reasonableness test to determine whether all optical scan ballots in a precinct were scanned and scanned only once. This test would compare the number of returned absentee ballots multiplied by the average number of sheets per ballot to the total number of scanned sheets. While these totals will not match exactly because of variation in the number of sheets per ballot, a large discrepancy would indicate either deleted or double-counted decks of ballots.

Recommendation 5

An audit similar to this, comparing electronically recorded optical scan results to those obtained by hand counted examination of the optical scan ballots, should be performed after every election and before certification.

In general, the results of the counts corresponded closely in this audit. There was, however, a very low frequency of lower votes recorded by the electronic system. There is no reason to expect this to bias a race vote count but it does suggest that further verification of the accuracy and completeness of the optical scanning system under real world conditions is needed.

IV. Security, Accuracy, and Sufficiency of the Data Needed for Auditing

When the Collaborative Audit Committee began its work, the presumption was that the tabulation data from the central tabulation computer (GEMS server) would be easily identifiable and readily made available to the Audit committee or Center for Election Integrity/Monitor staff engaged in audit work. This proved not to be the case.

A. GEMS Election Results: Tabulation Files and Reports

To conduct the audit, the Center's professional staff specified certain files in generic terms in writing. We received confirmation that the ballot department would be providing the files needed for the DRE audit immediately upon the closing of the unofficial tabulation on November 8. Although the Center went out of its way to have staff present throughout the 36 hour Election Day and Night to take possession of the GEMS reports needed and was present when the election closed early Wednesday afternoon, November 8, the data that the ballot department supplied did not satisfy the specifications and did not permit the audit to proceed.

The Center staff then undertook a series of conversations with CCBOE Director Michael Vu and with Diebold's technician Chris Bellis about how GEMS produces data and the types of files and reports that are possible after the election has closed. We then drew up a new list of the data files that were needed for the audit. If the information that we were given is correct, no single GEMS report is available that has exactly what is needed for both audits (absentee ballots and DREs). We discovered that a series of analytic steps using several types of election reports was required in order to obtain the data necessary to complete the audit.

Based on the information that we were able to obtain from the ballot department and the Diebold representative, we list in the accompanying footnote the data we required to complete the audit.[26] Despite our effort to pin down the exact data required and to ensure

[26] The electronic files or reports we apparently needed for this audit:

a. GEMS Statement of Votes Cast (SOVC) Report run on the database backup after absentee ballots were tabulated, but *BEFORE* DRE memory cards were uploaded.
b. Database file after absentee ballots were uploaded, but before GEMS tabulation was performed.
c. GEMS data export after absentee ballots were uploaded, but before GEMS tabulation was performed.
d. Database file after DRE uploading was complete.
e. GEMS data export after DRE uploading was complete.
f. GEMS SOVC Report after all absentee ballots performed on DREs.
g. Need the database file after all absentee ballots performed on DREs were uploaded.
h. GEMS data export after all absentee ballots performed on DREs were uploaded.

that we obtained the requisite files immediately after the election's unofficial count closed, we were unable to do so. The Ballot Department manager advised that the files turned over on November 8 included all that we had requested and needed, even though they did not.

B. Reliability and Accuracy of the Data from the GEMS Computer

Inconsistent absentee ballot results files. For the absentee ballot audit, the ballot department provided several different electronic files that should have had the same data but actually reported different election results. It is unclear to us, and apparently to the CCBOE as well, why these election results files differ (see Appendix 13). We have no independent knowledge of which results file should be used or why GEMS generates a variety of files with varying election totals. What is clear to us, however, is that it is critical for the ballot department to have accurate information on which file contains the actual total election results. It is also essential information for determining the degree of fidelity the audit hand-count has to the electronically produced election results.

Raw election data and database review. The Monitor software engineers sought to review the raw election data to compare it with the GEMS-reported results to determine if there were any errors in the GEMS tabulation.[27] Additionally, certain tabulation events (i.e., server crashing during scanning operations; freezing of the database during a backup and compression operation) occurred during the unofficial count that raised the possibility of database corruption.

The CCBOE Director initially would not permit the raw election data to be provided to the Audit committee or to the Monitor. He said Diebold Election Systems, Inc. (DESI) would assert trade secret or other protection of this data as proprietary. We challenged the legal basis for any such claim.[28] Eventually, a limited database review was conducted by Monitor software engineers with a DESI representative present and several CCBOE ballot and information services managers. Focusing on only three of the November races, the lead engineer showed the observers that for each of the three, GEMS maintained two separate election results tables that held values that were inconsistent with one another. The results differed between the two tables by over 100 votes for each of the three races checked.

---

[27] Joe Hall of the UC Berkeley School of Information provided significant consultation as the Monitor prepared for this database review and served as a sounding board for other technical questions.

[28] We find that the decision in *Assessment Technologies v. Wiredata*, 350 F. 3d 640 (2003) (Posner, J.) (concerning real estate tax assessment data) persuasively demonstrates that the election voting data would be beyond propriety control if urged to be protected by copyright law. We thank Professor Mike Madison of the University of Pittsburgh Law School for bringing this case to our attention. For a discussion of trade secret claims asserted by voting system vendors and possible challenges to those claims, see: Aaron Burstein, Stephen Dang, Galen Hancock and Jack Lerner, "Legal Issues Facing Election Officials in an Electronic-Voting World", Samuelson Law, Technology and Public Policy Clinic at the University of California at Berkeley School of Law (Boalt Hall), available at: http://www.law.berkeley.edu/clinics/samuelson/projects_papers/Legal_Issues_Elections_Officials_FINAL.pdf

We filed a written query with DESI, and received a response that we find raises more questions (see Appendix 14). In brief, the GEMS software engineer said that the tables are updated at different points and that this does not matter to the final results. This explanation did little to alleviate our concerns. Additionally, we have no clarity on which table contains the final accurate results.

The Monitor's software engineers conducting the review also found other strong indicators of possible database corruption, including blank fields. (See Appendix 16 for a memo on other database corruption indicators). Microsoft's JET engine, which DESI used to communicate with the vote tally database, is documented to have a problem with unpreventable database corruption.[29] (See Appendix 17 for excerpts from a Microsoft publication concerning security and corruption issues in the JET platform.)

→An in-depth Monitor's Report on technical and database issues is forthcoming.

C. Hardware and Software Design Impediments to Auditing

Hardware design issues: The current generation of major brand optical scanners, including those used in Cuyahoga County, do not count *ballots* but only ballot *pages*. In Cuyahoga's General Election in November 2006, among the 59 separate jurisdictions, optical scan ballots could vary in length by several pages. Also, voters did not always return every page of the ballot when they sent it in. Thus, even if we know the total number of optical scan ballots that the CCBOE received for tabulation, we have no easy way to determine whether all the ballots were part of the tabulation. To determine whether all the ballots had been counted, the CCBOE executives simply averaged the number of ballot pages and *estimated* that all the optical scan ballots had been counted.

This design problem also impedes the ability to produce accurate undervote rates (in specific races or ballot issues).

By contrast, with punch cards the CCBOE was able to determine with complete accuracy whether all the ballots that had been received had been counted. The current generation optical scan hardware (and firmware) design, however, does not include features that are essential to determining whether all ballots are counted. As a result of new, apparently HAVA-compliant[30] equipment, we have reduced rather than increased the accuracy and reliability of our elections results. This reduction in reliability is apparently due to an engineering design omission, one that must be redressed either by a hardware change or expensive auditing procedures.

Software Design Issues The GEMS system currently does not report election data at the DRE unit level of specificity. The lowest level of reporting is for the precinct. This means that the accuracy of particular DRE machines cannot be determined via an audit.

---

[29] *How to Troubleshoot and to Repair a Damaged Access 2002 or Later Database*, (Rev. 6.1 2006) *at* http://support.microsoft.com/default.aspx?scid=kb;en-us;283849.

[30] The Help America Vote Act, 42 USC SS 15301-15545.

D. Security: Logging and Data Systems in the CCBOE

As stated in the *Monitor's Report on Possible Legal Noncompliance* (January 8, 2007),[31] the Ballot and Information Services Departments have failed to implement crucial Security Policy provisions that are designed to protect the tabulation server and the integrity of the election results. The paper and ink logs that were to be used to record deleted ballot batches and server events were largely unutilized, in violation of the Security Policy, and probably one of the key reasons for the inability to track deleted batches to assure their re-scanning.

E. Recommendations for CCBOE Action

1. Obtain independent guidance (to supplement and compare that from DESI) on what electronic files should be used for each type of election auditing, and how the files differ from one another.
2. To permit accurate election audits to be conducted, the Secretary of State should specify the data that must be kept and for what period of time.

3. The CCBOE Board should authorize the Monitor to ascertain whether the security policy has been fully implemented and to provide recommendations for how to achieve full compliance before the next election.

4. A citizen's advisory board of up to five qualified individuals should be created to focus on technical and security issues. Its first task, in conjunction with the Monitor, should be to review, rewrite, and improve the CCBOE Security Policy.

5. The CCBOE should request an independent evaluation of the GEMS database from a qualified consultant. The task should be to ascertain whether database corruption occurred in the November 2006 election. Secondly, the consultant should make recommendations on how to avoid database corruption to the maximum extent feasible and what steps should be taken to protect election data as tabulations are occurring.

V. TOP TIER RECOMMENDATIONS for SYSTEMIC IMPROVEMENT

This report covers many audit findings in great detail but it is by necessity limited in scope. Budget, timing, and legal and administrative impediments narrowed the scope of the two audits to such a degree that they do not provide a comprehensive view of how Cuyahoga County's overall election system is functioning. While we believe our findings are extremely important and merit strong consideration by the CCBOE, they are not a stopping point. They are a first step in providing public oversight of the electoral system.

[31] The *Public Monitor Report on Possible Legal Noncompliance* (dated Jan. 8, 2007) can be found at www.csuohio.edu/cei/.

1. <u>Independent random audits should be a routine part of the election process.</u>

Auditing is standard business practice and should be applied to our voting systems because of their importance. There is clear evidence that problems exist:

- This Collaborative Public Audit has discovered problems with DRE Long Reports and the Optical Scan counting process;
- As reported in the Cleveland *Plain Dealer* in November 2006, thousands of people voted without having signed in at the polling place;
- Two CCBOE employees were convicted for performing illegal actions during the 2004 recount; and
- The ESI audit and Cuyahoga Election Review Panel assessments after the May 2006 election found numerous problems (e.g., 9.6% of paper audit trails, including the legal ballots, were defective or compromised the audit).

A reasonable approach might be to perform an independent audit after each major election and a collaborative internal audit after smaller local elections. The time and cost involved do not need to be exorbitant and will decrease as problems are resolved and process controls are put in place. A periodic professional independent audit could help identify needed improvements and restore voter confidence in the system. Future election audits should include evaluations of the following issues so that internal administrative and technical systems may be improved where needed:

- Electronic voting & legal ballots (e.g., do the paper ballots/VVPATs match the electronic counts?)
- Chain of custody of election materials (e.g., were security procedures followed?)
- Provisional ballot procedures (e.g., Did the right people cast these ballots? How many voters lost their vote because they were at right polling location, but were not directed to the correct precinct?)
- Optical Scan/Absentee ballots (e.g., were all the ballots counted? Were they counted accurately? Were any ballots counted more than once?)
- Security Plan (e.g., was the plan complete? Was the plan implemented?)
- Internal Controls (e.g., were important internal processes documented? Were those procedures followed?)

In addition to implementing a routine comprehensive professional audit, the Collaborative Audit Committee believes the current system, which relies upon two voting systems, should be seriously reviewed.

2. Reconsider the feasibility and wisdom of supporting two major voting systems –Optical Scan and DREs.

The problems found in this audit, the ESI audit, and report from the Cuyahoga Election Review Panel[32] call into question whether it is practical and cost effective for Cuyahoga County to support two voting machine systems (i.e., electronic and optical scan). Some factors to be considered include:

- **Election Costs for 2006 went well beyond the budget.** Some costs were one time costs, but a significant amount of the overrun was for enhanced training to help prepare poll workers and Election Day Technicians (EDTs) for an increasingly complicated job. These costs probably will not go away because we cannot assume that these workers will return and remember the complex instructions that they were taught a year ago.

- **It is unclear if DRE electronic voting can support the turnout in a Presidential election.** Despite a large increase in absentee voting for November 2006, a federal judge ordered 16 polling places to be kept open after the normal closing time of 7:30 PM because of reported wait times exceeding one hour. The voting turnout in a presidential year is substantially higher than a mid-term election. What planning has occurred to avoid problems with lines in 2008? Have options other than purchasing more DRE units been considered for dealing with the expected spike in turnout?

- **CCBOE staff must be hired and trained to support both systems.** Hardware needs to be set up, poll worker manuals need to be provided, poll worker and professional staff training must be planned and executed, and different types of ballots and pre-election and post-election testing must be prepared and executed. All of this needs to be done for two systems instead of one. Does the CCBOE have the resources (including managerial and financial) to achieve success with two systems?

- **The DREs present considerably more hurdles to complete auditing than do optical scanning systems.** The problems with the DRE printers causing damaged Long Reports, and the difficulties in locating data printed in a miniscule typeface on a narrow register-receipt that can be over 20 feet long, are only two impediments to DRE auditing.

If the CCBOE claims that continuing to use two voting systems is the best solution, the burden of proof should on the CCBOE to show:

- That they will resolve the problems reported in the CERP report, the ESI audit, and January 8, 2007 Monitor memo from the Center For Election Integrity;
- That they have or will hire the managers and staff necessary to resolve the problems caused by staff shortages; and

[32] The Cuyahoga Election Review Panel's Final Report can be found at www.csuohio.edu/cei/ (dated July 20, 2006). This webpage provides the option of reading or downloading the panel report in separate chapters rather than in its entirety of 400 pages (including appendices).

- The difference between maintaining two voting systems (including poll worker training, vendor support costs, and CCBOE staff headcount and expenses) and a single optical scan voting system is a defensible cost.

3. Undertake a GEMS election results Database Integrity and Reliability Evaluation

The Diebold Corporation used a Microsoft database "engine" (JET) as the foundation for its GEMS software. Microsoft has posted warnings that database corruption cannot be completely prevented in this "engine." Microsoft also warned that JET was inappropriate for use where there were high needs for data accuracy and security. (See Appendix 17) The risk factors for GEMS data integrity can be identified. The CCBOE should examine, using a qualified expert, the integrity of the November 2006 GEMS database and solicit recommendations for minimizing the risks to the accuracy and integrity of election tabulations.

4. Evaluate the Voter Registration Software System

While analyzing the feasibility of supporting two voting systems, we also recommend an assessment of the DIMS voter registration system. While not part of this audit, DIMS was repeatedly mentioned by both internal CCBOE staff and external observers as a weak link within the electoral system. Both the January 8, 2007 *Public Monitor Report on Possible Legal Noncompliance* and the December 7, 2006 memo from Tom Hayes of the LNE group (serving as the CCBOE's Program Manager) to the Cuyahoga County Commissioners[33] describe a number of problems with DIMS including: lost voter records due to overwriting, corrupted poll worker applicant information, inconsistencies in the voter history record, and lost productivity due to the need to reboot the system several times each day. The CERP Final Report[34] devoted almost an entire chapter to the DIMS voter registration database problems but reportedly no investigation has ever been conducted. The range of problems has increased. A technical evaluation to identify the design and operational problems, and any "glitches," is warranted so that the problems can be fixed or the system replaced. Maintaining an arguably defective voter registration database may present legal liability for the CCBOE as well.

* * *

This Collaborative Audit Committee appreciates the authorization to conduct this audit and would look forward to working with the CCBOE's new managerial and Board Member team to improve election verification and other internal controls.

[33] Memo from Tom Hayes, LNE Group to the Cuyahoga County Board of County Commissioners (December 7, 2006), p 1.

[34] CERP Final Report, see www.csuohio.edu/cei/ at chapter 1-2.

Appendices

Appendix 1

Background on the Cuyahoga Collaborative Public Audit:

Creation, Purposes, Authority, and Participants in the Collaborative Public Audit

I. The Need to Achieve Independent Verification of Election Results

Achieving accuracy in reported election results is the primary objective for any quality election administration. Given the range of recent information reported nationally about possible problems with e-voting technologies, and also some of the problems the Cuyahoga County Board of Election (BOE) experienced in prior elections, election reform organizations and the major political parties sought to have the local election results independently verified as accurate reflections of the ballots cast in the November 2006 election. In early fall, the chief initial public concerns focused on the DRE touchscreen voting devices which were to be used at polling places on election day.

After discussions with election reform organizations about their concerns, the Public Monitor of Cuyahoga Election Reform[1] introduced at a public Board meeting a proposal for a Collaborative Public Audit. The proposal pledged that the Monitor would seek the cooperative involvement of the local Democratic and Republican Parties, plus several election reform organizations to conduct the independent audit. The audit, per the reform organizations' requests, was to focus on the Diebold DRE touchscreen voting machines. The DRE units are the primary technology used in Cuyahoga County for Election Day voting at the polling locations. The DRE units are also used in "walk-in" absentee voting.[2]

The BOE Board Members unanimously approved the DRE audit proposal (and one other presented in the same verification proposa) on October 2, 2006, noting that some flexibility might be needed and that the Board's attorney needed to approve its legality. Thereafter, the county political parties' chairmen (Republican and Democratic) requested that the audit be extended to include optically scanned absentee ballots. The Audit Committee, which had been formed and begun working, agreed to this extension. The CCBOE Board Members unanimously approved the extension as well.

The Collaborative Audit participants believe the public wants independent verification that the election results that the e-voting technology has generated are accurate. Additionally, they believe both the election administrative staff and the public at large need to know whether the voting machines' programming maintained its integrity after the machines passed the pre-election testing and were deployed to the polling locations for Election Day. Reliable information on these and other questions are crucial so that sound decisions can be

[1] The Center for Election Integrity of Cleveland State University per a proposal and testimony prepared by its Director, Candice Hoke.
[2] Functionally, "walk-in" absentee voting is a form of early voting.

made as to the voting and database technologies we used and so that any corrections in administrative or other systems that are needed can be identified. While the audits that were conducted are limited rather than comprehensive and conclusive on these points, the information acquired is useful on these and other issues.

A national Election Audit Workgroup teaming the Brennan Center with with the Samuelson Law, Technology & Public Policy Clinic at Boalt Hall School of Law (UC Berkeley), as well as several election officials and leading academics as been working to evaluate current audit laws and procedures and provide critical analysis to public officials as they begin to adopt audit schemes and procedures. The workgroup has thus far identified five core goals that should motivate the design of election auditing: increasing public confidence in the results of an election; deterring fraud against the voting system; detecting large-scale systemic errors; providing feedback that will allow jurisdictions to improve elections and machinery in future years, and confirming to a high level of confidence that a 100% manual recount would not change the outcome of the race.

We agree strongly with this statement of election auditing design goals but would add a sixth: providing additional incentives for the staff to reach higher standards of accuracy. In order to achieve these six and other auditing goals, we have concluded, as has the Election Audit Workgroup, that the independence of the auditing entity is essential.[3]

The Collaborative Audit Committee commends the Cuyahoga Board of Election for taking this Ohio leadership role in initiating election auditing and thus creating an independent mechanism for verifying the announced election results. We would also like to thank the over forty volunteers that gave their time over numerous days to help conduct this audit. Without this huge volunteer effort, this audit would not have been possible.

Policy Formation, Structure, and Participating Entities

The participating organizations that exercised policymaking powers over the audit and solicited volunteers were:

- Democratic Party of Cuyahoga County
- Republican Party of Cuyahoga County
- League of Women Voters
- CASE-Ohio (Citizens' Alliance for Secure Elections)
- Greater Cleveland Voter Coalition

[3] Lawrence D. Norden, Statement to the U.S. House of Representatives, Committee on House Administration, Subcommittee on Elections, March 20, 2007 at 2; Candice Hoke, Statement to the U.S. House of Representatives, Committee on House Administration, Subcommittee on Elections, March 20, 2007 at 2 (this testimony to the Subcommittee on Elections that held hearings on Federal Election Auditing can be found at http://www.verifiedvotingfoundation.org/article.php?id=6445).

The Center for Election Integrity at CSU, in its role as Public Monitor for Cuyahoga County Board of Elections, served as the coordinator of the audit process. Center staff undertook a great deal of auditing duties but proposed the audit structure so that it acted as a neutral facilitator rather than a policymaker with a vote in Collaborative Audit group decisions. The Center for Election Integrity supplied professional staff services. Assistant Director Abigail Horn led the Center's audit work.

The policy decisions governing the audit, including which races to audit, were made by the representatives of the participating policymaking organizations. Each participating organization was limited to a maximum of two representatives on the planning and policymaking Audit Committee. The political parties sent experienced professional auditors and lawyers. The election reform organizations supplied individuals with a wide range of election expertise, including software engineers with technical voting technology expertise and poll workers or election observers. Virtually all decisions were made by consensus.

CSU's Northern Ohio Data Information Service (NODIS)[4] directed by Dr. Mark Salling designed the sample and audit methodology and provided analysis of the results.

[4] http://nodisnet1.csuohio.edu/nodis/index.shtml

Appendix 2

Methodology and Procedures to Select Sample for Cuyahoga County Election Audit of DRE Long Reports versus GEMS Tabulations

Prepared by
Ellen Cyran and Mark Salling
Northern Ohio Data and Information Service
Maxine Goodman Levin College of Urban Affairs
Cleveland State University

December 28, 2006

This report describes the methodology used to select the sample of precincts used in the audit of the printed long reports produced from the electronic voting machines (DRE) immediately after the polls close on Election Day.[5] This audit is to verify the accuracy of the long reports against the published output of GEMS tabulation system that is produced after loading data from each of the memory cards used by the DREs.[6]

To insure that any discrepancy found is unlikely to affect the outcome of an election, the sample size is based on the closest race among those selected for inclusion by the collaborative audit group. The audit group selected county or statewide races with each political party selecting a race and civic groups selecting the third race. The unofficial election results, which included electronic voting machines (DRE) at the polling locations and early absentee optical scanned ballots, were used to determine the closest race. If the race was a statewide race, then the margin between the candidates at the state level was used in addition to the county level to determine the closeness of the race.

The steps involved in determining the sample size are as follows.

1. Calculate the percentage vote margin between the top two candidates of the closest race. In this case, the three selected races had only two candidates each.
2. Since the closest race was a statewide race and the statewide percent winning margin was less than the county-wide margin, the statewide margin percentage was used. The resulting margin was 2.1 percent of the votes cast for that race (state auditor).
3. Apply the state percentage vote margin (2.1%) to the votes in the county for the selected race, divide by two, and add one to obtain the votes needed to change the winner of the race. This provides the number of votes in the county that need to be switched in order to change the outcome of the race, assuming that the percentage margin is applied uniformly statewide.
4. Assume a maximum vote shift of 15 percent between the leading candidate and all other candidates in any precinct. (The Brennan Center recommends 7.5 percent for polling

[5] Multiple DREs may be (are often) used at each polling place to collect votes on one or more precincts.
[6] This audit is performed since the long reports are available for audit soon after the election. The voter-verified paper audit trail (VVPAT) is not available for the audit because Ohio state law bars access to it.

location sampling and 15 percent for voting unit sampling.[7] This value represents the estimated maximum proportion of votes per polling location, precinct, or voting machine that needs to be switched for a candidate in order to change the outcome of the race.)

5. Sort precincts by descending order of votes cast in the closest race using the unofficial results reported from the Cuyahoga County Board of Elections tabulation server (based on voting from the DREs at the polls and the early absentee results).
6. Calculate the vote shift per precinct:
   a. Sort the precincts in descending order by votes cast in the closest race.
   b. Apply the 15 percent vote shift rate to each precinct, rounding up to the nearest vote. The 15 percent vote shift rate is from one candidate to another or 30 percent vote shift margin.
   c. If the winning candidate did not receive 15 percent of the votes in any given precinct, then assign a zero vote shift for the precinct.

   This would total to the necessary votes to change the election result (if applied uniformly across the state).
7. Sum the vote shift amount among the precincts until reaching (or just exceeding) the number calculated in step three; i.e., the number of votes necessary to change the outcome. The count is the minimum number of corrupt votes to alter the election with a 2.1 percent margin difference. The number of precincts, which were required to obtain the minimum number of corrupt votes, is the minimum number of corrupt precincts required to alter the election.
8. Use a hypergeometric distribution to determine the probability P of selecting at least one corrupt precinct in a sample of s precincts selected from a population of N precincts containing b corrupt precincts. The formula is:

$$P = 1 - \frac{\binom{N-b}{s}}{\binom{N}{s}}$$

   This formula must be solved for s with a computer program[8] or by estimation. A computer program was used since it gives the most accurate result. The formula was solved to determine the number of precincts that must be audited to insure 95 percent and 99 percent confidence interval levels.
      a. The 99 percent confidence intervals requires 110 precincts
      b. The 95 percent confidence intervals requires 72 precincts;
9. Add 20 percent to the sample size to account for "long reports" that may not be available or useable. Since the 99 percent confidence level was preferred, 22 secondary or "back-up" precincts were added to the primary 110 precincts to be drawn in the sample. Thus,

---

[7] The Brennan Center Task Force on Voting System Security, Lawrence Norden, Chair, *The Machinery of Democracy: Protecting Elections in an Electronic World*, pg 22, http://www.Brennancenter.org/dynamic/subpages/download_file_39288.pdf.

[8] A Matlab program was converted to SAS to calculate the sample size, based on the minimum corrupt votes and the number of corrupt precincts from step 7. The Matlab program is available from Dopp, Kathy and Stenger, Frank: "The Election Integrity Audit," National Election Data Archive Project, September 25, 2006, http://electionarchive.org/ucvAnalysis/US/paper-audits/ElectionIntegrityAudit.pdf.

110 precincts are needed to achieve the objectives, though a total of 132 precincts are to be drawn.

The following steps were then used to select the sample precincts.

10. Select a sampling seed. Single-digit numbers submitted by each member of the audit collaborative were used to construct the seed.
11. Obtain the overall sample ($s_{overall}$=132) with 'proc surveyselect' in SAS®[9] from the population of N = 1,434 precincts.
12. Using the same seed as was used in the overall sample selection, obtain the primary sample ($s_{primary}$ = 110) with 'proc surveyselect' in SAS® from the overall sample of useable forms ($s_{useable}$), where $s_{useable}$ is expected to be between 110 and 132.
13. Sort the 110 primary sample precincts and the 22 secondary sample precincts separately in descending order by votes cast in the largest precinct and polling location. This kept selected precincts at the same polling place together in the listing to facilitate data collection from the long reports. It also insured that the largest precincts were examined first and included in the sample in the event that a complete sample could not be implemented.

[9] SAS®, http://www.sas.com.

Appendix 3
Example of the Form for Recording DRE "Long Report" Data

Recorder: _____ Reviewer: _____ Start Date: _____ Time: _____ End Time: _____

	Polling Place Name	Precinct Name	DRE Serial Number	Report OK - not torn, missing, incomplete (Yes, No)	Precinct Name matches Report (Yes, No)	Report signed (Yes, No)	Total Votes Cast	Judicial		Auditor	Supreme Court		Reviewed?	Comment
								Gallagher	Hastings	Sykes	O'Neill	O'Donnell		
1	1410-ST. SAVA CHURCH HALL B	BROADVIEW HEIGHTS -03-												
2	1410-ST. SAVA CHURCH HALL B	BROADVIEW HEIGHTS -03-												
3	1410-ST. SAVA CHURCH HALL B	BROADVIEW HEIGHTS -03-												
4	1410-ST. SAVA CHURCH HALL B	BROADVIEW HEIGHTS -03-												
5	1410-ST. SAVA CHURCH HALL B	BROADVIEW HEIGHTS -03-												
6	1410-ST. SAVA CHURCH HALL B	BROADVIEW HEIGHTS -03-												
7	1410-ST. SAVA CHURCH HALL B	BROADVIEW HEIGHTS -03-												
8	1410-ST. SAVA CHURCH HALL B	BROADVIEW HEIGHTS -03-												
9	1410-ST. SAVA CHURCH HALL B	BROADVIEW HEIGHTS -03-												
10	1410-ST. SAVA CHURCH HALL B	BROADVIEW HEIGHTS -03-												
11	1410-ST. SAVA CHURCH HALL B	BROADVIEW HEIGHTS -03-												
12	1410-ST. SAVA CHURCH HALL B	BROADVIEW HEIGHTS -03-												
13	1410-ST. SAVA CHURCH HALL B	BROADVIEW HEIGHTS -03-												
14	1410-ST. SAVA CHURCH HALL B	BROADVIEW HEIGHTS -03-												
15	1410-ST. SAVA CHURCH HALL B	BROADVIEW HEIGHTS -03-												
16	1410-ST. SAVA CHURCH HALL B	BROADVIEW HEIGHTS -03-												

Appendix 4
Basic Statistics on DRE Long Report entries

General:

1. The complete sample contained 1,414 unique long reports. The BOE had 5,834 DREs to use on Election Day (although it is unclear if they used them all). If all the available DREs were used, our sample represented 24.2 percent of all long reports.
2. The complete sample contained 132 precincts in 121 polling locations. This represents 9.2 percent of all precincts in the county.
3. The precincts in the complete sample contained 32,062 total votes cast. This represents 8.9 percent of the total votes cast in the county (361,025).
4. In the long report sample, 246 unique long reports (some containing data for more than one precinct in our sample) were not audited at all because those precincts/polling locations were missing some long reports. Without a complete set of long reports for a given precinct, we were unable to audit the existing long reports.
5. This leaves 1,168 unique long reports audited and used in the frequency counts. Some of these long reports contained data for more than one precinct in our sample.

Race and total vote matches:

1. 95 precincts matched the GEMS Server for total votes casts and the six candidate total in the three races.
2. Six precincts partially matched the GEMS Server data since the long reports were missing for some of the races audited. The two listed below matched at least one complete race. The other four precincts matched at least one candidate, but not a complete race.

    - Lakewood 3-E, polling location 5650-Westerly Apts. (Barton Ctr) matched in total, state auditor and Supreme Court races. DRE SN 295434 had a tape jam so the results for judicial race were missing for that DRE.

    - East Cleveland 3-D, 4810-Martin Luther King Civic Center matched only the judicial race. DRE SN 254353 was blank for the other races.

3. 31 precincts did not match because of problems with long reports in those polling location.

Appendix 5
Duplicate DRE Serial Numbers

1. Two duplicate DREs with different vote counts were found within polling locations.

   DRE SN 278596 – Garfield Heights 1D, Polling location 8027-St. Timothy Manor

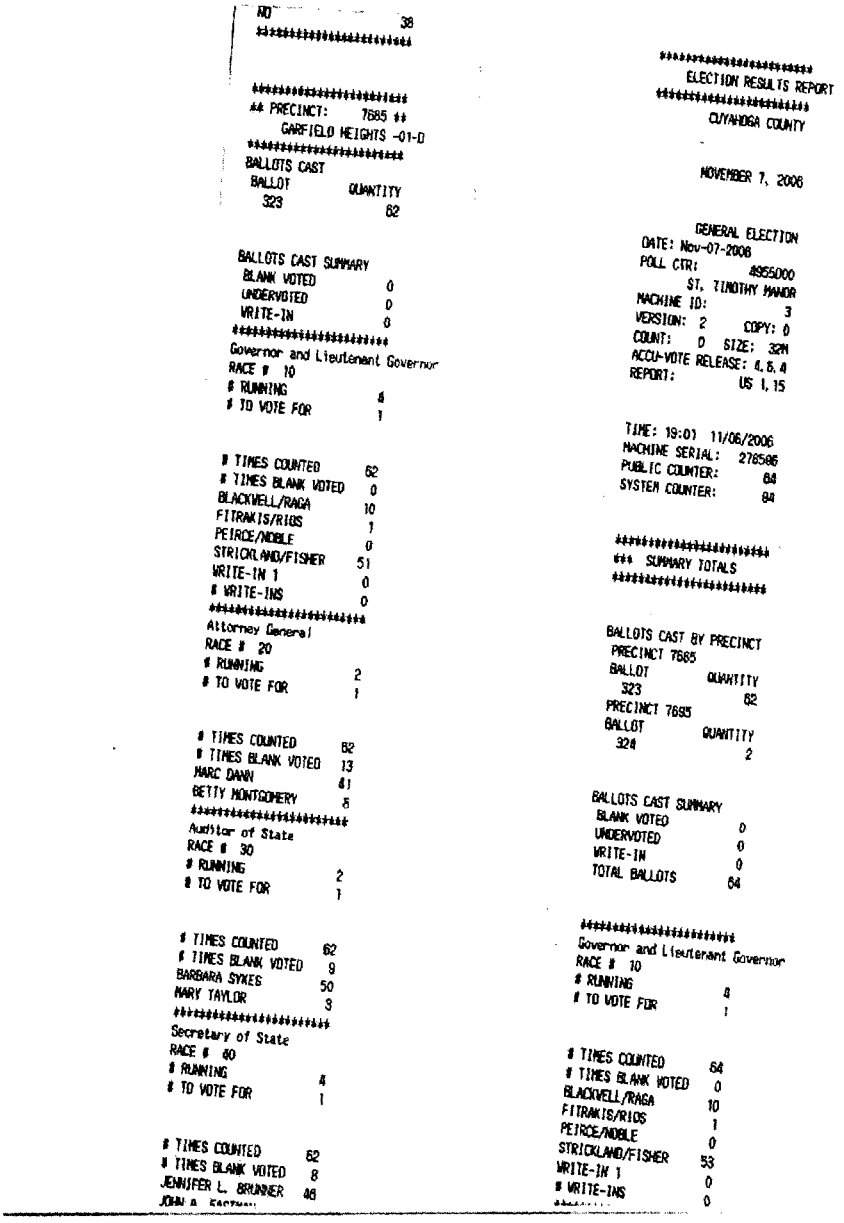
   DRE SN 254886 – Middleburg Heights 4D Polling location 6100-Baptist Mid-Missions

   None of the above duplicates were deleted from any reporting. The votes in both duplicate long reports appears to have been loaded into the GEMS server since both are needed for the totals to match the audit totals.

2. One duplicate DRE across polling locations was found.

   DRE SN 260368 - Brook Park 1E, Polling location 1460-Brook Park Recreation Center
   Cleveland 3Q, Polling location 2261-Church Of God Of Cleveland

Appendix 6
2 DREs from the Same Precinct with the Same Serial Number:
Photocopies of Excerpts of 2 Long Reports
(note right column portion, "*MACHINE SERIAL*")



AD 38

PRECINCT: 7685
GARFIELD HEIGHTS -01-D

BALLOTS CAST

BALLOT	QUANTITY
323	62

BALLOTS CAST SUMMARY

BLANK VOTED	0
UNDERVOTED	0
WRITE-IN	0

Governor and Lieutenant Governor
RACE # 10
RUNNING 4
TO VOTE FOR 1

# TIMES COUNTED	62
# TIMES BLANK VOTED	0
BLACKWELL/RAGA	10
FITRAKIS/RIOS	1
PEIRCE/NOBLE	0
STRICKLAND/FISHER	51
WRITE-IN 1	0
# WRITE-INS	0

Attorney General
RACE # 20
RUNNING 2
TO VOTE FOR 1

# TIMES COUNTED	62
# TIMES BLANK VOTED	13
MARC DANN	41
BETTY MONTGOMERY	8

Auditor of State
RACE # 30
RUNNING 2
TO VOTE FOR 1

# TIMES COUNTED	62
# TIMES BLANK VOTED	9
BARBARA SYKES	50
MARY TAYLOR	3

Secretary of State
RACE # 40
RUNNING 4
TO VOTE FOR 1

# TIMES COUNTED	62
# TIMES BLANK VOTED	8
JENNIFER L. BRUNNER	46
JOHN A. [illegible]	

ELECTION RESULTS REPORT
CUYAHOGA COUNTY

NOVEMBER 7, 2006

GENERAL ELECTION
DATE: Nov-07-2006
POLL CTR: 4955000
ST. TIMOTHY MANOR
MACHINE ID: 3
VERSION: 2 COPY: 0
COUNT: 0 SIZE: 32M
ACCU-VOTE RELEASE: 4.6.4
REPORT: US 1,15

TIME: 19:01 11/06/2006
MACHINE SERIAL: 278586
PUBLIC COUNTER: 64
SYSTEM COUNTER: 84

SUMMARY TOTALS

BALLOTS CAST BY PRECINCT
PRECINCT 7685

BALLOT	QUANTITY
323	62

PRECINCT 7685

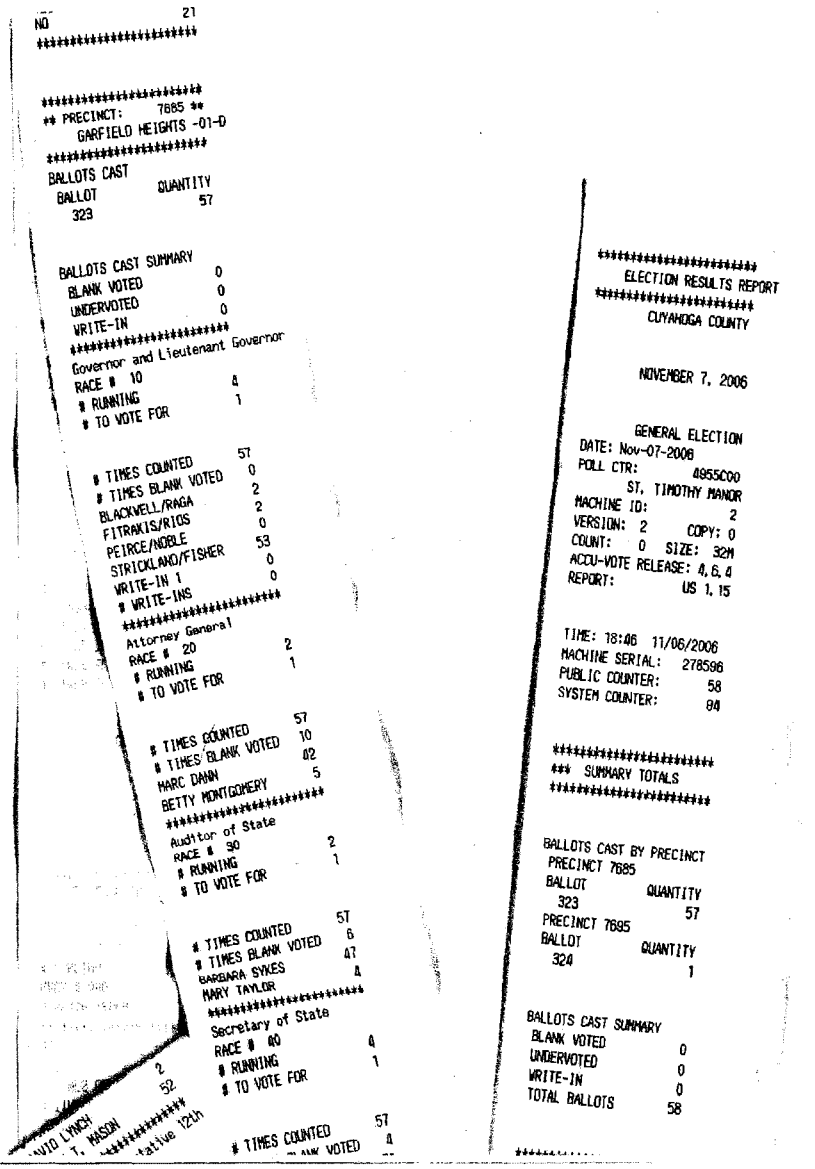
BALLOT	QUANTITY
324	2

BALLOTS CAST SUMMARY

BLANK VOTED	0
UNDERVOTED	0
WRITE-IN	0
TOTAL BALLOTS	64

Governor and Lieutenant Governor
RACE # 10
RUNNING 4
TO VOTE FOR 1

# TIMES COUNTED	64
# TIMES BLANK VOTED	0
BLACKWELL/RAGA	10
FITRAKIS/RIOS	1
PEIRCE/NOBLE	0
STRICKLAND/FISHER	53
WRITE-IN 1	0
# WRITE-INS	0



NO 21

**PRECINCT: 7685 **
GARFIELD HEIGHTS -01-D

BALLOTS CAST
BALLOT QUANTITY
323 57

BALLOTS CAST SUMMARY
BLANK VOTED 0
UNDERVOTED 0
WRITE-IN 0

Governor and Lieutenant Governor
RACE # 10 4
RUNNING 1
TO VOTE FOR 1

TIMES COUNTED 57
TIMES BLANK VOTED 0
BLACKWELL/RAGA 2
FITRAKIS/RIOS 2
PEIRCE/NOBLE 53
STRICKLAND/FISHER 0
WRITE-IN 1 0
WRITE-INS 0

Attorney General
RACE # 20 2
RUNNING 1
TO VOTE FOR 1

TIMES COUNTED 57
TIMES BLANK VOTED 10
MARC DANN 42
BETTY MONTGOMERY 5

Auditor of State
RACE # 30 2
RUNNING 1
TO VOTE FOR 1

TIMES COUNTED 57
TIMES BLANK VOTED 6
BARBARA SYKES 47
MARY TAYLOR 4

Secretary of State
RACE # 40 4
RUNNING 1
TO VOTE FOR 1

TIMES COUNTED 57

ELECTION RESULTS REPORT
CUYAHOGA COUNTY

NOVEMBER 7, 2006

GENERAL ELECTION
DATE: Nov-07-2006
POLL CTR: 4955C00
ST, TIMOTHY MANOR
MACHINE ID: 2
VERSION: 2 COPY: 0
COUNT: 0 SIZE: 32M
ACCU-VOTE RELEASE: 4,6,4
REPORT: US 1,15

TIME: 18:46 11/06/2006
MACHINE SERIAL: 278596
PUBLIC COUNTER: 58
SYSTEM COUNTER: 84

*** SUMMARY TOTALS

BALLOTS CAST BY PRECINCT
PRECINCT 7685
BALLOT QUANTITY
323 57
PRECINCT 7695
BALLOT QUANTITY
324 1

BALLOTS CAST SUMMARY
BLANK VOTED 0
UNDERVOTED 0
WRITE-IN 0
TOTAL BALLOTS 58

Appendix 7. All Unmatch d Precincts

Id	First Line	Polling_Place_Name	Precinct_Name	Difference (Audit minus GEMS)							Partial Matches	Comments
				Votes Cast	Gallagher	Hastings	Sykes	Taylor	O_Neill	O_Donnell		
1	31	50-BROOK PARK RECREATION CENTER	BROOK PARK -01-E	-81	-34	-20	-49	-30	-28	-37	no	Missing parts of long reports
2	157	3980-CLEVELAND KOREAN PRESB. CHURCH	CLEVELAND -16-P								no	Missing several long reports
3	158	3980-CLEVELAND KOREAN PRESB. CHURCH	CLEVELAND -16-Q								no	Missing several long reports
4	189	5400-GATES MILLS COMMUNITY HOUSE	GATES MILLS -00-B								no	All long reports missing for this precinct
5	201	7220-ST. MARGARET MARY CHURCH HALL	SOUTH EUCLID -01-C	-17	-9	-2	-8	-7	-8	-7	no	Missing several long reports
6	228	1120-BEACHWOOD HIGH SCHOOL	BEACHWOOD -00-F								no	Missing several long reports
7	295	6700-JOHN MUIR ELEMENTARY SCHOOL	PARMA -04-A	-3	0	-3	-2	-1	0	-2	Partial, but not the same race	Missing one long reports
8	308	1170-COLUMBUS INTERMEDIATE SCHOOL	BEDFORD HEIGHTS -03-C								no	Missing several long reports
9	458	6090-MIDDLEBURG HTS. CHURCH OF GOD	MIDDLEBURG HEIGHTS -04-A	-277	-74	-100	-94	-137	-70	-128	no	Missing several long reports
10	464	7830-ST. JUDE PARISH HALL	WARRENSVILLE HTS -07-B								no	Missing several long reports
11	516	7580-HIGH POINT RECREATION CENTER	STRONGSVILLE -02-I	-1	-11	-24	0	-1	0	-1	Partial, but not the same race	Torn long reports
12	571	4990-OUR LADY OF LOURDES SHRINE	EUCLID -04-B								no	Missing several long reports
13	698	3012-ZION CHAPEL(MISS BAPT ANNEX)	CLEVELAND -01-U	-24	-12	-1	-17	-2	-8	-9	no	Missing several long reports
14	718	6130-ST. WENCESLAS SCHOOL	MAPLE HEIGHTS -04-C								no	Missing several long reports
15	719	6130-ST. WENCESLAS SCHOOL	MAPLE HEIGHTS -04-D								no	Missing several long reports
16	773	3040-CUDELL RECREATION CENTER	CLEVELAND -18-I								no	Missing several long reports
17	796	5650-WESTERLY APTS. (BARTON CTR)	LAKEWOOD -03-E	0	-5	-2	0	0	0	0	Partial	Printer jam couldn't read two races
18	842	8024-FIFTH CHRISTIAN CHURCH	CLEVELAND -01-B	-2	0	-1	-2	0	0	-1	Partial, but not the same race	precinct missing on long report
19	916	2440-ST. MARTIN DEPORRES CENTER	CLEVELAND -09-K								no	Missing several long reports
20	936	5710-LINCOLN ELEMENTARY SCHOOL	LAKEWOOD -02-H	-190	-58	-74	-101	-72	-79	-79	no	Missing several long reports
21	937	5710-LINCOLN ELEMENTARY SCHOOL	LAKEWOOD -02-I	-6	-2	-1	-6	0	-3	-3	Partial, but not the same race	Missing several long reports
22	980	4220-GLENVILLE HIGH SCHOOL	CLEVELAND -09-E	-189	-71	-47	-162	-8	-79	-71	no	Missing 1 long reports
23	985	4860-TERRACE TOWERS	EAST CLEVELAND -04-E								no	Missing several long reports
24	990	2265-BOYS & GIRLS CLUB OF CLEVELAND	CLEVELAND -03-L								no	Missing several long reports
25	1013	2420-CAPTAIN ARTHUR ROTH SCHOOL	CLEVELAND -09-F								no	Missing several long reports
26	1027	6535-SENIOR CITIZENS CENTER BLDG-G	OAKWOOD -06-A	-83	-36	-12	-61	-14	-32	-23	no	printer problems
27	1097	4500-SIMPSON UNTD METHODIST CHURCH	CLEVELAND -18-R								no	Missing all long reports
28	1107	4280-IMMACULATE HEART OF MARY	CLEVELAND -12-D	-37	-14	-17	-24	-9	-13	-19	no	Missing 1 long report
29	1153	6710-RIDGEBROOK ELEMENTARY SCHOOL	PARMA -01-G								no	Missing several long reports
30	1194	2360-EVERLASTING BAPTIST CHURCH	CLEVELAND -10-J								no	Missing 1/2 of a long report
31	1206	4810-MARTIN LUTHER KING CIVIC CENTER	EAST CLEVELAND -03-D	-17	0	0	-12	-2	-11	-3	Partial	Blank tape for auditor and supreme court
32	1328	6580-ORANGE VILLAGE HALL	ORANGE -00-C	-11	-4	-13	-5	-4	-5	-5	no	Missing 1 long report
33	1380	8016-PEARLBROOK CHURCH OF GOD	CLEVELAND -16-S								no	Missing all long reports
34	1419	2300-ALEXANDER G. BELL ELEM. SCHOOL	CLEVELAND -06-S	-58	-28	-12	-50	-3	-43	-35	no	Missing 1 long report
35	1527	2080-GREATER ABYSSINIA TOWERS	CLEVELAND -08-O								no	Missing several long reports
36	1546	4290-WESTSIDE SACHSENHEIM HALL	CLEVELAND -16-A								no	Missing several long reports
37	1547	4290-WESTSIDE SACHSENHEIM HALL	CLEVELAND -16-C								no	Missing several long reports

Note: Those precincts with blanks (no differences recorded) did not have completed audits because long report problems were identified at the beginning and auditors knew they would not have sufficient information to do a comparison with GEMS data.

Appendix 8
Discrepancies between PDF and sum of CSV files for unofficial results
(128 precincts)

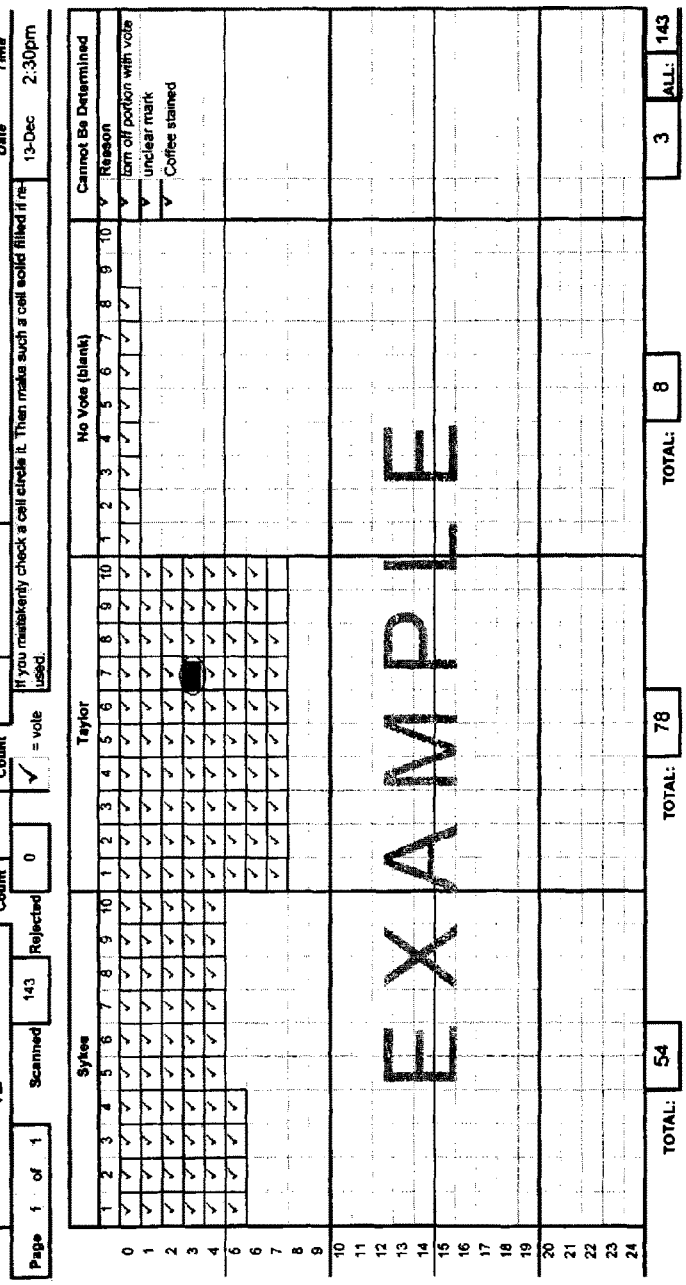
	Difference - Unofficial PDF results minus combined CSV results						
Precinct	Cards Cast	Sykes	Taylor	Gallagher	Hastings	O'Donnell	O'Neill
BEACHWOOD -00-D	1	0	0	0	1	0	1
BEACHWOOD -00-H	1	1	0	0	1	1	0
BEACHWOOD -00-K	1	1	0	1	0	0	1
BEDFORD -01-A	1	1	0	0	0	1	0
BEDFORD -03-A	3	2	1	2	0	0	1
BEREA -02-A	1	0	1	0	1	1	0
BRECKSVILLE -00-E	2	0	1	0	2	2	0
BRECKSVILLE -00-L	1	0	0	0	0	0	0
BROOKLYN -00-A	1	0	1	0	1	0	1
BROOKLYN -00-C	2	1	0	1	0	1	1
BROOKLYN -00-F	1	1	0	1	0	0	1
BROOKLYN -00-G	2	2	0	1	1	1	1
BROOK PARK -01-A	1	1	0	1	0	0	1
BROOK PARK -01-B	1	0	1	0	1	1	0
BROOK PARK -01-C	1	1	0	0	0	0	0
BROOK PARK -02-A	1	0	1	0	1	0	1
BROOK PARK -02-C	1	0	1	0	1	1	0
BROOK PARK -04-A	1	0	1	0	1	1	0
CLEVELAND -01-D	1	1	0	0	1	0	1
CLEVELAND -01-F	1	1	0	1	0	0	1
CLEVELAND -01-N	1	1	0	1	0	0	1
CLEVELAND -01-P	1	1	0	0	0	0	1
CLEVELAND -02-A	1	1	0	0	0	1	0
CLEVELAND -02-I	1	1	0	0	0	0	1
CLEVELAND -02-S	5	5	0	0	1	0	2
CLEVELAND -03-B	1	1	0	0	1	1	0
CLEVELAND -03-R	1	0	0	0	0	0	0
CLEVELAND -05-J	1	0	1	1	0	1	0
CLEVELAND -05-L	1	1	0	1	0	0	1
CLEVELAND -05-M	1	1	0	0	0	1	0
CLEVELAND -05-N	1	1	0	0	0	0	0
CLEVELAND -05-R	1	1	0	1	0	0	1
CLEVELAND -08-E	1	1	0	1	0	0	1
CLEVELAND -08-R	1	0	0	0	1	1	0
CLEVELAND -09-F	1	1	0	1	0	1	0
CLEVELAND -09-G	1	1	0	1	0	0	1
CLEVELAND -09-J	1	1	0	0	0	1	0
CLEVELAND -09-K	1	1	0	0	0	0	1

CLEVELAND -10-M	1	1	0	1	0	0	0
CLEVELAND -10-Q	1	1	0	1	0	1	0
CLEVELAND -11-J	2	1	0	1	0	1	0
CLEVELAND -13-E	1	1	0	1	0	1	0
CLEVELAND -13-X	1	1	0	0	0	0	0
CLEVELAND -15-E	1	1	0	0	1	1	0
CLEVELAND -16-D	1	1	0	1	0	1	0
CLEVELAND -16-Q	1	0	1	0	0	0	0
CLEVELAND -16-R	1	1	0	0	0	0	1
CLEVELAND -17-G	1	0	1	0	1	0	1
CLEVELAND -18-D	1	1	0	1	0	1	0
CLEVELAND -19-C	1	1	0	0	0	0	1
CLEVELAND -19-D	2	2	0	0	0	0	2
CLEVELAND -20-A	1	0	0	0	0	0	0
CLEVELAND -20-N	1	0	0	0	0	0	0
CLEVELAND -21-A	1	0	1	1	0	1	0
CLEVELAND -21-G	1	0	1	1	0	1	0
CLEVELAND -21-P	2	2	0	0	2	0	2
CLEVELAND HEIGHTS -01-J	2	1	1	0	1	0	1
CLEVELAND HEIGHTS -04-D	1	1	0	1	0	0	1
EAST CLEVELAND -03-G	1	0	1	0	1	0	1
EUCLID -01-D	2	0	2	0	2	1	1
EUCLID -01-M	1	1	0	1	0	0	1
EUCLID -03-K	1	0	0	0	1	0	0
EUCLID -04-D	1	0	1	1	0	0	1
EUCLID -04-I	1	1	0	1	0	0	1
GARFIELD HEIGHTS -01-E	1	1	0	1	0	1	0
GARFIELD HEIGHTS -02-C	1	1	0	1	0	0	1
GARFIELD HEIGHTS -05-C	1	0	0	0	0	0	0
INDEPENDENCE -00-A	1	1	0	1	0	0	1
INDEPENDENCE -00-G	1	0	1	0	1	0	1
INDEPENDENCE -00-H	1	1	0	0	0	0	0
LAKEWOOD -01-A	2	0	2	0	0	0	1
LAKEWOOD -01-L	1	1	0	1	0	0	1
LAKEWOOD -02-K	1	1	0	0	1	1	0
LAKEWOOD -04-D	1	1	0	1	0	1	0
LYNDHURST -02-D	1	1	0	1	0	0	1
LYNDHURST -03-A	1	1	0	0	1	1	0
LYNDHURST -04-E	1	0	1	0	1	1	0
MAPLE HEIGHTS -03-D	1	0	1	1	0	0	1
MAPLE HEIGHTS -04-A	1	1	0	1	0	0	1
MAPLE HEIGHTS -04-C	1	1	0	1	0	0	0
MAPLE HEIGHTS -07-C	2	1	1	2	0	1	1
MAYFIELD HEIGHTS -00-B	1	0	1	0	1	0	1

MAYFIELD HEIGHTS -00-F	2	1	0	1	0	0	1
MAYFIELD HEIGHTS -00-M	1	1	0	1	0	0	1
MAYFIELD VILLAGE -01-A	1	0	1	0	1	1	0
MAYFIELD VILLAGE -03-A	1	0	1	0	1	1	0
MIDDLEBURG HEIGHTS -04-C	1	1	0	0	1	0	1
NEWBURGH HEIGHTS -00-A	1	0	0	1	0	0	0
NORTH OLMSTED -01-B	1	0	1	0	1	1	0
NORTH OLMSTED -02-D	1	1	0	1	0	0	1
NORTH OLMSTED -04-A	2	1	1	2	0	1	1
NORTH OLMSTED -04-G	1	1	0	0	0	1	0
NORTH OLMSTED -04-H	1	1	0	0	1	0	1
NORTH ROYALTON -03-A	1	0	1	0	1	1	0
NORTH ROYALTON -03-E	2	0	1	0	2	1	0
NORTH ROYALTON -05-C	1	0	1	0	0	1	0
OLMSTED TOWNSHIP -00-B	2	1	1	0	1	0	1
PARMA -01-C	1	1	0	0	0	0	0
PARMA -01-E	1	1	0	1	0	0	1
PARMA -02-A	1	1	0	0	0	0	0
PARMA -03-A	1	1	0	1	0	0	1
PARMA -03-J	1	1	0	1	0	0	1
PARMA -04-C	1	1	0	1	0	0	1
PARMA -05-D	1	1	0	1	0	0	1
PARMA -06-D	1	0	1	0	1	1	0
PARMA -07-G	1	0	1	0	0	0	1
PARMA -08-E	1	0	1	0	1	1	0
PARMA -09-E	1	1	0	1	0	0	1
PEPPER PIKE -00-B	1	1	0	0	1	0	1
PEPPER PIKE -00-D	1	0	1	0	1	0	1
PEPPER PIKE -00-F	3	2	1	1	2	0	3
ROCKY RIVER -02-F	2	1	1	1	1	1	1
ROCKY RIVER -03-B	1	0	0	0	1	1	0
SEVEN HILLS -01-C	1	1	0	1	0	0	1
SEVEN HILLS -03-C	1	1	0	1	0	0	1
SHAKER HEIGHTS -00-JJ	1	0	0	0	1	1	0
SOLON -01-C	1	0	1	0	1	0	1
SOLON -02-B	1	1	0	0	0	0	1
SOLON -03-C	1	1	0	0	0	0	0
SOUTH EUCLID -02-G	1	0	0	0	0	0	0
STRONGSVILLE -04-C	1	0	0	0	0	0	0
UNIVERSITY HEIGHTS -00-F	1	1	0	1	0	1	0
UNIVERSITY HEIGHTS -00-M	2	2	0	1	1	0	2
WESTLAKE -02-C	1	0	0	0	0	0	0
WESTLAKE -02-D	1	1	0	1	0	1	0

WESTLAKE -04-B	1	1	0	0	1	0	1
WESTLAKE -05-E	1	0	1	1	0	1	0
WESTLAKE -05-F	1	0	1	0	0	0	0
Total	152	91	42	58	50	48	72
Maximum difference	5	5	2	2	2	2	3
Minimum difference	1	0	0	0	0	0	0

Appendix 9 **Form (example) Used to Audit the Optical Scan Ballots**



Appendix 10
Discrepancies in Optical Scan Hand Count from GEMS report

Group A. The audit hand count results were **lower** than the GEMS reported count in these 16 precincts:

Beachwood 0-E	*-1 Sykes*	
Berea 4-C		*-1 Taylor*
Brook Park 1C	*-1 Sykes*	
Brook Park 2A		*-1 Taylor*
Cleveland 14-J	*-1 Sykes*	
Cleveland 17-B	*-1 Sykes*	
East Cleveland 4-H	*-3 Sykes*	
Mayfield Heights 0-1	*-1 Sykes*	
North Olmstead 1-A	*-1 Sykes*	
North Olmstead 4G	*-1 Sykes*	
Olmsted Falls 3-A	*-2 Sykes*	*-2 Taylor*
Richmond Heights 3-C		*-1 Taylor*
Shaker Heights 0-Q	*-1 Sykes*	
South Euclid 2-A	*-1 Sykes*	
University Heights 0-E	*-1 Sykes*	
Westlake 2-B	*-1 Sykes*	

Group B. The audit hand count results were higher than the GEMS reported count in these 11 precincts:

Broadview Heights 1-D	*+1 Sykes*	*+1 Taylor*
Broadview Heights 2-C	*+1 Sykes*	
Cleveland 3-K	*+1 Sykes*	
Cleveland 6-D	*+1 Sykes*	
Cleveland 7-T	*+1 Sykes*	
Cleveland 11-D	*+1 Sykes*	
Highland Hills 0-A	*+1 Sykes*	*+1 Taylor*
Lyndhurst 4-C	*+1 Sykes*	
Maple Heights 4-D		*+1 Taylor*
Rocky River 3-B	*+1 Sykes*	
Seven Hills 4-B		*+1 Taylor*

Group C. The audit hand count results were both higher and lower for the candidates compared to the GEMS reported count in precinct Lyndhurst 1-B with –1 Sykes vote and +1 Taylor vote.

Group D. The GEMS reported count was zero ballots counted and zero votes in precinct North Olmsted 2-F. The folder for OS ballots for this precinct contained ballots (36 for Sykes, 21 for Taylor, and 3 blank).

Appendix 11
Investigation of Discrepancies in Optical Scan Audit

Discrepancy Evaluation – Group A

Examination of the Central Count report for information about the 16 precincts with discrepancies of a lower count (Group A) showed that 11 of the precincts had ballot cards filed in an additional location. Such ballot cards would have been included in the GEMS count but because they were not present in the folder at the time of the audit, they would not have been included in the audit tabulation. There appear to be two subgroups in this category. One group has additional ballot cards misfiled as a minor component of another deck in numbers consistent with the numbers of votes missing, i.e., three ballot cards per vote.

Specifically

Beachwood 0-E	*1 missing vote*	*3 ballot cards wrong deck*
Cleveland 14-J	*1 missing vote*	*3 ballot cards wrong deck*
East Cleveland 4-H	*3 missing votes*	*9 ballot cards wrong deck*
Mayfield Heights 0-1	*1 missing vote*	*3 ballot cards wrong deck*
North Olmstead 1-A	*1 missing vote*	*3 ballot cards wrong deck*
Olmsted Falls 3-A	*4 missing votes*	*12 ballot cards wrong deck*
Richmond Heights 3-C	*1 missing vote*	*3* ballot *cards wrong deck*
Shaker Heights 0-Q	*1 missing vote*	*3 ballot cards wrong deck*

The second group has single ballot cards scanned in a deck that consisted of only that single card. The origin of these single card decks is not known.

Specifically

Brook Park 1C	*1 missing vote 1 ballot card solo deck*
Brook Park 2A	*1 missing vote 1 ballot card solo deck*
North Olmstead 4G	*1 missing vote 1 ballot card solo deck*

These ballot cards were not recovered from their locations nor examined to determine votes marked. The number of ballot cards in all cases was sufficient to account for the number of votes that were missing from the respective precincts.

The discrepancies in the other five precincts in Group A could not be explained by this means since there was no evidence found of ballot cards filed in locations other than the folder examined by the audit.

Discrepancy Evaluation – Group B

Examination of the Central Count report for information about the 11 precincts with discrepancies of a higher count (Group B) showed that six of the precincts had additional ballot cards from other precincts included. These would not have been included in the GEMS count but could possibly have been included in the audit tabulation if they were not recognized and excluded.

Specifically:

Broadview Heights 1-D	*2 extra votes*	*4 cards other precincts*
Broadview Heights 2-C	*1 extra votes*	*3 cards other precincts*
Cleveland 6-D	*1 extra votes*	*3 cards other precincts*
Highland Hills 0-A	*2 extra votes*	*6 cards other precincts*
Lyndhurst 4-C	*1 extra votes*	*3 cards other precincts*
Rocky River 3-B	*1 extra votes*	*3 cards other precincts*

During a second follow-up visit to the BOE, these precinct folders were re-examined specifically to determine if the ballot cards from other precincts shown by the Central Count to be present were in fact present and to determine if these ballots had been included in the audit count. In all six of these precinct folders, ballot cards from other precincts were indeed present. In three folders, the original audit count had apparently included the misfiled ballot cards and the discrepancy was resolved when these were excluded. In the other three precincts, the misfiled ballots had apparently been excluded at the time of the original audit (the misfiled ballots were all placed first in each folder) and the re-count results excluding these were the same as those found in the original audit.

The discrepancies in the other five precincts in Group B could not be explained by this means.

Group C - Other Discrepancy Evaluation

The one precinct (Group C; Lyndhurst 1-B) in which the audit count was one vote high for one candidate and one vote low for the other was also recounted and the results were found to be the same as the original audit count.

NOTE: During this follow-up visit, five other precincts with discrepant results that were not apparently explained or reconcilable by misfiled ballots were examined and re-counted. In all cases the counts were the same as those from the initial audit.

Appendix 12
Precincts with All or Most Optical Scan Ballots Missing from GEMS

Because we had by chance selected a precinct (North Olmsted 2F) that had OS ballots returned but not recorded in the Central Count Report or on the SOVC report we were aware that this was a possible explanation for no results and no ballots counted. An alternate explanation for zero results would be if there were, in fact, no absentee ballots returned for these precincts. In an attempt to determine if that was the case we determined the number of absentee ballots reported returned for each of these precincts by November 3, 2006, the cutoff time for inclusion in the early absentee scanning. This file was obtained from the BOE (absentee voters for November 2006.csv). Nine of the 11 precincts did not have any absentee ballots returned, but two others did.

As a follow-up, the report of absentee ballots returned was compared to the number of ballots reported in the GEMS report and ballots counted in the Central Count report for all precincts.

Within the limitations of the data and possible errors in the absentee information it appears likely that all or nearly all of the ballots for at least several precincts were not included in the unofficial SOVC. Specifically:

Chagrin Falls Twp A	*126 voters 11 abs returned*	*0 SOVC*
Cleveland 2I	*940 voters 30 abs returned*	*1 SOVC*
Cleveland 13X	*920 voters 12 abs returned*	*1 SOVC*
North Olmsted 2F	*759 voters 63 abs returned*	*0 SOVC*

We asked to examine these four decks and were able to examine three of them. One was not able to be found and was not present on the log showing storage location. The documentation on the folders for the three decks examined indicated that these ballots had been scanned during the unofficial count. One of these had a notation "Reject delete" that had been erased but was still readable. It appears that these precincts were deleted from the GEMS tally for some reason. The precinct folders examined contained ballots in numbers corresponding to the number of absentee ballots reported returned.

The procedure during scanning for the unofficial count required verification by the tabulation staff that the number of pages reported on GEMS was within a certain margin of error of the number of pages reported by the scanner. If not within that margin of error the tabulation staff was to delete the batch result from GEMS and the deck was to be rescanned. In these cases, it is possible that after deleting the digital batch from GEMS, the ballots were not rescanned but simply put back in the file. Two precincts each showed one vote in GEMS because there was a single ballot card for each of those precincts present in a deck that consisted of only the single card.

Appendix 13
BOE Email on Missing Batch in the Unofficial Count

-------- Original Message --------
Subject: Missing Batch in the Unofficial Count
Date: Fri, 29 Dec 2006 13:28:30 -0800 (PST)
From: Frank James Hlad <fjhlad@yahoo.com>
To: Abigail Horn <abigail@urban.csuohio.edu>

We have no evidence of that missing batch in the unofficial count. As we said, it looks as if the batch was scanned, deleted from GEMS, and never re-scanned. Austin had that printout that Kurt was talking about, and the precinct showed no votes cast.

We have been unable to find transaction log information on that day. I am not certain if that's because Matt and Brian don't know where to look or if the log doesn't exist. We did locate a transaction log from the official count, but there was no way to sort or find data within it. It is massive, as you might imagine.

I guess I don't know what to tell you about all this. Your point about dropping a batch in the official count is well taken. Because we can't output data in any usable form from GEMS, we really have no mechanism (except eyeballs) to catch a problem like that. F

Appendix 14
Differences between files provided by the BOE for Optical Scan Audit

run date	Title in PDF	Name of File	Received by Audit	Cards Cast	Sykes	Taylor
11/13/2006 (12:48 PM)	Post Absentee/Pre DRE	gems sovc report post avos - pre tsx.pdf	11/13/2006	201,290	40,194	21,059
11/13/2006		post avos- pre tsx data.csv	11/13/2006	201,290	40,194	21,059
11/27/2006 (7:52 AM)	filename Official, but data is unofficial, inside the document only titled ABS	GEMS SOVC REPORT official AVOS only 11-06.pdf	1/31/2007	201,595	40,321	21,068
1/31/2007 (10:54 AM)	ABS, Unofficial Results	GEMS SOVC REPORT Unofficial AVOS Only.pdf	1/31/2007(?)	201,473	40,307	21,109

Appendix 15
Email Exchange between the Monitor and DESI about GEMS Database

-------- Original Message --------
Subject: Database Question posed by the Monitor
Date: Fri, 17 Nov 2006 16:28:21 -0500
From: Bellis, Chris <BellisC@diebold.com>
To: Michael Vu <bempv@cuyahogacounty.us>, Lou Irizarry <belmi@cuyahogacounty.us>, Matthew Jaffe <bemij@cuyahogacounty.us>, Hiner, Jessica <jessicah@dieboldes.com>, Candice Hoke <shoke@law.csuohio.edu>, tryan@law.csuohio.edu
CC: Gwen Dillingham <begdx@cuyahogacounty.us>, Green, Pat <GreenP@diebold.com>

Earlier today as a result of the Monitor's Investigation of a GEMS Database [a Monitor software engineer] ran the following SQL statement on a mdb file off of a CD:

SELECT SUM(Vote Totals) from candidatecounter WHERE CANDVGROUPID = 1433

The resulting value was 186,205.
Then he ran the following statement on the same .mdb file

SELECT SUM(Vote Totals) from sumcandidatecounter WHERE CANDVGROUPID = 1433 AND VCENTERID <> -1

The resulting value was 186, 027.

Two questions emerged:
1. Why is the value different?
2. Why do we store candidate totals in two different tables?

ANSWER:

Chris,
The SumCandidateCounter table is used to store the totals by precinct rather than by counter batch; this was done for performance reasons. The SumCandidateCounter table is updated from the CandidateCounter table when a report is printed whereas the CandidateCounter table is updated when the when the results are posted. Therefore if results had been posted since the last report was printed the totals would not match.
Hope this helps.

Tab

Talbot Iredale, P.Eng,
Software Development Manager
Diebold Election Systems

Appendix 16
Indicators that MAY Show Database Corruption
(Discovered in the Monitor's Review of CCBOE *Unofficial* Results Database on 11/17/06)[10]

1. Table element entries were missing date/time stamps of when the information was entered.

2. Table element entries had date/time stamps of January 1, 1970, which is the epoch (zero-point) of UNIX time.

3. In an email dated November 3rd, 2006, from DESI's Talbot Iredale, he claimed

> "Accounting for transaction overhead, I do not expect the database to grow by more than 100 MB during absentee processing. However this will vary dependent on what other other activities (printing, reports, etc.) occur during the processing."

The database grew to a size greater than 100 MB for absentee processing and a size above 1000 MB for the full election. What happened? Why were the estimations wrong? Precision is very important, especially when dealing with votes. Where else were DESI calculations imprecise?

4. Vote totals in two separate database tables held different values. DESI has provided a response, but as of yet, this response has not been tested or verified.

5. In an email from Chris Bellis dated Monday, November 20, 2006, Mr. Bellis summarized the "large amount of concurrent activity" that was occurring on the GEMS server on election night. This included DRE uploads, the JResults server running, the AVServer running, and Digital Guardian running, all interacting with the database in varying functions. In a subsequent email from Jessica Hiner, dated Sunday, November 26, 2006, Ms. Hiner stated "In the context of an online system with many users, Jet would not be an appropriate choice, but that is not how we use it."

- It appears in DESI's own words, Hiner acknowledges that when there is a large amount of concurrent activity, Jet database corruption can occur. Chris Bellis has said that on election night, there was a lot of concurrent activity on the server. Taking these two statements together, it would seem very possible that corruption may have occurred.

Microsoft's own documentation has stated that database corruption within JET is unavoidable. This statement is without qualifiers. Normal operation of the Jet database includes corruption.

---

[10] *From a Monitor staff software engineer with substantial database expertise who conducted an initial review of the unofficial election results database with representatives of DESI and the BOE present; the Monitor's review was limited to just over one hour. T resulting information was provided to Project Director Candice Hoke, who then hand-delivered it to the Board Members at the November 2006 certification Board meeting.*

Appendix 17
Excerpt from Microsoft Documentation on JET-Access Databases
(emphasis added)

Security

Although Access databases (using the Jet engine) can be password protected and encrypted, ***these databases do not have the same level of security*** as SQL Server or mainframe database systems. ***If data security is critical***, a SQL Server solution is the better choice.... SQL Server allows distributed data in a controlled and highly secure manner.

Data Integrity

Similarly, ***data integrity and recovery is not as robust on file-based databases using Jet....***

File server ***databases using Jet may become corrupt*** and require regular maintenance to maintain optimal results. ***Even with maintenance, the chance of failure is much higher*** than with SQL Server. ....

Transaction Logs and Rollbacks

If you need to know who modified what data, and undo changes, SQL Server's built-in features and triggers support this *[but not Access using JET—ed.]*

An Access application can try to replicate the tracking of changes by managing user interaction with the data. However, it would require programming and could not be managed at the core data level. ***Mistakes in the application or other applications in contact with the Access data could cause data changes that are not documented.*** There are ***also no rollbacks*** *[opportunities to "undo" the operation—ed.]* ***in Access after a transaction is committed.***

The above paragraphs can be found in *Microsoft Access or SQL Server: What's Right in Your Organization?* at
http://www.microsoft.com/sql/solutions/migration/access/compare-access.mspx

MARCH 2007

electionline.org

Briefing

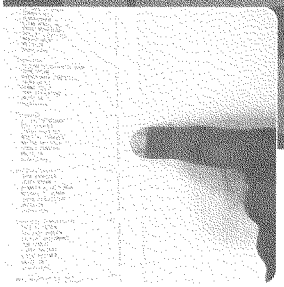


Photo courtesy Tom Courbat, Election Defense Alliance

Inside

FYI

Case Study: Auditing the Vote

In the five years since the passage of the Help America Vote Act, the American election process has been significantly changed with new machines, new procedures and modernized voter lists.

Still lacking, however, is the complete confidence of the voting public.

New machines are in place, but can they be trusted? Voters with disabilities can cast ballots secretly and independently, but can they verify their choices in the same fashion as everyone else?

Along with machine certification, testing and increased polling-place security, another tool to boost voter confidence is the use of post-election audits. But their use – as well as other procedures to elevate voter confidence – is disparate across the country.

While hand counts of ballots are nothing new – California has been conducting some form of machine audits since the 1960s – concerns over electronic voting technology have created a new urgency to ensure impartial verification of largely computerized voting technology.

This, the 17th *electionline Briefing*, explores the issue of post-election audits in a number of states. Like so many other issues in election

administration, the study finds that rules governing the practice vary greatly across borders as does the size of the sample, public access and scrutiny and response to disparities between vote counts and audit findings. While one state might require that 5 percent of all precincts audit ballots by hand, another might require a review of election-related procedures, including polling-place activities logged on machines, "zero tapes" from the start of the day and final tallies to make sure the counters tabulated results correctly.

Similarly, the impact of audits can vary substantially.

Nevada's audit of voter-verified paper audit trails (VVPATs) tests to see whether machine counts of electronic ballots and manual or mechanical counts of paper records match. If they do not, the electronic count is considered the vote of record. In neighboring California, the opposite is true – the paper count takes precedence over the electronic one.

There is also a wide variety of state rules governing the extent of audits. Connecticut performed the nation's most comprehensive post-election audit, counting 20 percent of precincts using optical-scan machines during a pilot program involving a few dozen jurisdictions. A bill pending in the legislature would make the practice state law beginning in 2008, at which time all jurisdictions will use the optical-scan systems.

Utah and California, in contrast, hand count ballots from 1 percent of voting machines and 1 percent of precincts, respectively.

And then there are the consequences for discrepancies. Wisconsin makes voting system manufacturers accountable for potential machine errors. Nevada has no stated remedy for differences in machine and hand counts, while California and a number of other states mandate that, if there are discrepancies, audits are expanded.

With such a wide variety of machines in use around the country – and an entrenched tradition of state and local authority over election administration – it comes as no surprise that yet another aspect of elections finds such varied approaches across borders. But that could change soon, perhaps before Americans head to the polls in 2008.

A bill introduced by U.S. Rep. Rush Holt, D-N.J., would add significantly more uniformity to post-election auditing. If approved, it would require not only the use of voter-verified paper audit trails, but the hand counting of the paper slips (or other forms of paper ballots) after elections. According to the bill, the number of ballots audited would vary based on the closeness of a race, ranging from as few as 3 percent of all precincts in some races to as many as 10 percent of precincts in close races.

Executive Summary

The U.S. election system has been re-fitted in recent years with federal requirements for new voting systems, statewide voter registration databases, provisional ballots and other Congressionally-mandated rules.

But voter confidence remains an issue. Post-election audits, during which machine totals from electronic voting machines or optically-scanned paper ballots are hand-counted, re-checked or otherwise put under additional scrutiny are one tool increasingly being employed to assure candidates, voters and political parties of the integrity and transparency in the system.

As with many other issues in election administration, however, the ability of and interest in conducting audits varies by state. So too does the sample size, selection process and remedy in case of a discrepancy between initial totals and audit findings.

This case study examines audit rules and procedures in a number of states, focusing specifically on California, Minnesota, Nevada, Arizona and Connecticut. The five selected have contrasting state requirements and handle audits differently. In Minnesota, a "100 percent paper ballot" system allows for hand counting. Organizations including League of Women Voters and Citizens for Election Integrity were invited to observe the process. In Arizona, current law requires audits, but only if representatives from each party are present to participate. Last year's general election saw only five of the state's 15 counties perform audits because of no-shows by potential auditors.

Sample sizes vary greatly as well. While California's 42-year-old law requires audits of 1 percent of all precincts after an election, Connecticut's pilot program of optical-scan voting systems included an audit of 20 percent of all precincts, a sample size established by academics along with state officials.

Among the case study's other findings:

- Calls for voter-verified paper audit trails (VVPATs) have grown in state houses as well as in Congress. More than half the states now require the use of paper trails with electronic voting machines or paper-based voting systems; however, of those, only 15 require manual post-election audits. A bill under consideration in Congress (H.R. 811) would require every state to audit both VVPATs and other paper ballots after elections.

- Several states that do not require VVPATs employ their own version of post-election audits. Maryland requires an audit of election records and voting systems. Texas requires jurisdictions using paperless DRE machines to perform a hand count of ballots through an examination of ballot images.

- Florida officials conducted an audit of DRE machines following the troubled 2006 vote in Sarasota County where more than 18,000 ballots recorded no choice in a race for the U.S. House of Representatives. Critics say the re-examination of materials shed no new light on the unusually high percentage of under votes.

Key Findings

For many, the ambiguous results from Florida's 13th Congressional District in Sarasota County put on national display the problems with paperless direct-recording electronic (DRE) voting machines. The machines did not record more than 18,000 votes in the ultra-competitive race to replace former Secretary of State Katherine Harris, because of a machine problem, ballot design flaw, intentional under votes, or a combination of other reasons, depending upon whom is asked.

For Democrats, who took control of Congress but ultimately lost the seat in question, Sarasota's missing votes could be the impetus necessary to compel hand-countable paper records with each vote cast on a DRE.

"The most serious problem occurred in Sarasota, Fla., where there were 18,000 under votes in the Congressional election. At this time, officials have been unable to account for what happened to these votes because there is no independent record," said Sen. Dianne Feinstein, D-Calif., during a hearing of the Senate Rules Committee to evaluate electronic voting systems.[1] A state-ordered audit – met with skepticism from some advocates – found the voting machines worked, fingering ballot-design flaws as the likely culprit.

The move toward requiring DREs to have voter-verified paper audit trails (VVPATs) has gained traction nationwide in recent months. More than half the states now require VVPATs for touch-screen voting systems or paper-based ballot systems and several more are considering the same. But state legislation might not be necessary for paper trails to become law. On Capitol Hill, nearly 200 members of Congress co-sponsored a bill that would make VVPATs mandatory nationwide.

In the quest for greater transparency through more election scrutiny, however, adding VVPATs is only one step. Some experts say counting and comparing paper audit trails or optical scan ballots to an electronic record is an essential tool.

"An independent voter-verified paper trail without an automatic routine audit is of questionable security value. 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," stated a report from the New York-based Brennan Center.[2]

A small but growing number of states conduct random audits of election results, with sample sizes ranging from a few precincts to a proposal that would mandate local election officials hand count ballots from one out of five precincts to ensure voting system accuracy and accountability. It would also require the audits be conducted by state auditors and not chief election officials.

Currently, more than a dozen states require post-election random manual audits. In Congress, H.R. 811 proposed by Rep. Rush Holt, D-N.J., would require both VVPATs and random audits.

While audits undoubtedly create more responsibilities for election administrators already taxed with understanding new or recently-implemented voting systems, constantly changing polling place rules and locations and perennial shortages of poll workers, few have questioned their necessity.

In June 2006, the League of Women Voters passed a resolution endorsing the use of paper trails and mandatory audits. The resolution called for paper to be used in recounts, audited randomly in "selected precincts... in every election and the results [of the audit] published by the jurisdiction."[3]

R. Doug Lewis, executive director of the Houston-based Election Center, an organization representing election administrators from around the country, said in 2005 that some kind of auditability is necessary, though the list should not be limited to paper. "We recognize that transparency is needed," he told a Georgia newspaper. Forms could include a paper printout as well as an audio or video record or some other system.[4]

States with manual audit requirements

Fifteen states with paper-based ballot systems or electronic voting machines with VVPATs currently have laws or regulations requiring manual audits: Alaska, Arizona, California, Colorado, Hawaii, Illinois, Minnesota, Missouri, New Mexico, New York, North Carolina, Utah, Washington, West Virginia and Wisconsin.[5]

Seeking to avoid a vast hand-count of thousands of punch-card ballots, election workers [in Cugahoga County, Ohio] broke state law by pre-sorting the ballots to ensure they matched the final tally.

Connecticut does not mandate random manual audits – lever machines in place in most of the state during last year's federal election do not allow for them – but conducted one as part of a pilot program that introduced updated voting systems in 2006. Legislation is being considered to require post-election manual audits by 2008 when optical-scan machines will have replaced lever systems statewide.

Nevada, which conducted its first audit of DRE voting machines with VVPATs in 2004, requires either a manual or mechanical audit.

The Process

States requiring audits establish a time table for completion that ranges from a few days to several weeks after an election. All require comparing a random sampling of paper ballots or VVPATs containing specified races with electronic tabulations, though the "randomness" of ballot selection has sometimes been called into question.[6]

How many ballots are audited and how to handle discrepancies between machine totals and manual count totals varies from state to state.

States generally audit either a percentage of total ballots, precincts or voting machines. Minimum requirements range from Utah's audit of 1 percent of voting machines and 1 percent of precincts in California to 10 percent of precincts in Hawaii and 20 percent of precincts in Connecticut's 2006 general-election audit. For more details, see the snapshot of the states on page 12.

In at least eight states, if discrepancies are found, audits must be expanded to include more ballots.

Other states have different options. In Wisconsin, the State Elections Board orders the voting machine vendor to investigate irregularities and can suspend use of voting systems.

"The State Elections Board (SEB) staff will request that the vendor investigate and explain the reasons for any differences between the machine tally and the paper record tally. Should the vendor fail to provide a sufficient written explanation, including recommendations for preventing future occurrences within 30 days of notification, the SEB will suspend approval of all voting systems manufactured or serviced by the vendor in Wisconsin."[7]

Random selection of ballots

There is broad agreement among academics, policymakers, computer scientists and advocates that randomness is essential to effective audits.

The danger of non-random counts was plainly on display in Ohio three years ago.

An attempt to conduct a manual count of cherry-picked precincts in Cuyahoga County, Ohio by two election workers led to criminal convictions.

The candidate-requested recount of the 2004 presidential election was undertaken after Libertarian and Green Party Presidential candidates alleged irregularities and voter intimidation during the vote. In response, the state mandated hand counts for punch-card ballots from 3 percent of county precincts. If the hand counts did not match machine counts, then ballots from the entire county would be counted manually.[8]

Seeking to avoid a vast hand-count of thousands of punch-card ballots, election workers broke state law by pre-sorting the ballots to ensure they matched the final tally. "This recount was rigged, maybe not for political reasons, but rigged nonetheless," said Kevin Baxter, the special prosecutor brought in from Erie County, Ohio. "They did this so they could spend a day rather than weeks or months [recounting the ballots]."[9]

Legislation

At press time, legislation had been introduced in six states to require audits: Connecticut, Florida, Indiana, Maryland, Montana and New Jersey. Legislation has also been introduced in an additional four states to change current audit rules.

In Virginia, lawmakers stripped a provision of an election bill that would have mandated audits, angering a lawmaker who lost a bid for statewide office by a razor-thin margin.

"The bill is a half measure. I'll probably vote for it in committee, but it just makes me mad when they take the audit out. What's the verifiable paper trail all about?" said Sen. R. Creigh Deeds, D-Bath County, who lost a bid for state attorney general in 2005 by 360 votes.[10]

Other audit requirements

Several states perform other types of audits, including audits of the ballots of DRE machines without paper trails and more general post-election audits of the voting system or election records.

In Texas, which has a wide variety of voting systems including paperless DREs, officials in 2006 mandated a 1 percent random audit of electronic voting systems that involved checking machine tallies against stored ballot images. The process is defined by the state as a "manual" audit.

Kentucky, which currently uses paperless touch-screen voting machines, also has an audit requirement "of randomly selected precincts representing 3 percent to 5 percent of the total ballots cast in each election."[11]

In Virginia, lawmakers stripped a provision of an election bill that would have mandated audits, angering a lawmaker who lost a bid for statewide office by a razor-thin margin.

Maryland, another state using all paperless DREs, requires an audit of election records and logs from individual voting machines.

"After each election, local boards of election verify that the vote totals printed from the individual voting units match the reports generated by the central tabulator……the local boards of election also conduct a post-election audit to confirm the accuracy of the polling place reports. This includes auditing signed voter authority cards, precinct registers, other polling place forms completed by the election judges, and the official election results."[12]

In Florida, while audits are not required, Sarasota County was ordered to perform one after a race for Congress yielded an unusually high number of under votes. The audit of the county's paperless DRE voting machines faced criticism, partially for a lack of access to source code and other inner workings of the voting system.

"A significant problem in the Florida case…is the inability of candidates, their representatives or members of the general public to learn anything about what might have gone on inside those voting machines," testified Dan Wallach, associate professor of computer science at Rice University during a U.S Senate hearing on electronic voting.[13]

ES&S, the voting machine company in question, contended this information was a trade secret and a judge ruling on a lawsuit over access to the system's source code agreed.

California: The Quest for Audit Transparency

> "I've gained a lot of respect for how complicated it is to do good auditing."
>
> –David Dill, *VerifiedVoting.org*

Nearly half a century ago, California's legislature approved a manual count law that required the random selection of a subset of paper ballots to be counted publicly by hand in order to verify that the technology used to count the ballots was accurate and reliable.

The 1965 law calls for a public audit of 1 percent of precincts after every election. The precincts are chosen randomly by local elections officials. In addition, the law also requires that for each race not included in the initial group, one additional precinct is to be counted.[14]

Until 2001, California was one of only four states that required public auditing of election results.

With the introduction of direct-recording electronic (DRE) voting machines, some counties were unable to comply with the state's manual recount law because they did not use a voter-verified paper audit trail (VVPAT). To eliminate that problem, the legislature voted unanimously to mandate VVPATs in 2004. The legislature voted again in 2005 to strengthen the manual count law by requiring the use of VVPATs.[15]

Observers of the audit process in California have expressed concern over how counties conduct the counts. Kim Alexander of the California Voter Foundation and David Dill, a Stanford University computer science professor, questioned the randomness of samples used for audits after noting that many counties were picking which precincts to audit several days in advance of the count.

"It does compromise the process because people know in advance what is going to be audited," Dill said. "And that means that maybe mistakes won't be caught if someone wanted to cheat."[16]

They also stated only a few counties had written procedures for their audits. Dill and a team of researchers from ACCURATE, a multi-institution voting research center funded by the National Science Foundation, are working with election officials to come up with best practices for conducting an audit.[17]

After collaborating with ACCURATE during the audit of the June 2006 primary, Warren Slocum, San Mateo County's chief elections officer, included public participation in the random selection of precincts. Slocum has a member of the public roll three 10-sided dice — red, white and blue — with one side of each die corresponding to a precinct. [18]

He also had a webcam installed in the room where the audit was conducted so the public could watch the manual count on the Internet.

"San Mateo is aiming for the gold standard in the manual recount process," Slocum said. "We are establishing practices that will assure voters and election officials of the integrity of the vote."[19]

Members of ACCURATE also discovered that the mandate to certify an election within 28 days complicates the audit process.

"A particular challenge for San Mateo County – and they did a good job with this – was making sure that they didn't begin their manual audit process until all the votes were counted," wrote Joseph Hall, Ph.D. candidate in information economics and policy at the University of California, Berkeley, in an analysis.[20]

Elections officials and observers alike are hoping that state legislators take what was learned during the 2006 election cycle to heart and work to change and clarify some of the audit law to make the process more transparent and easier.

"I've gained a lot of respect for how complicated it is to do good auditing," Dill said.[21]

Minnesota: Building an Audit Consensus

Note: *The following section is a reprint from* electionline Weekly, *Dec. 14, 2006. Some information has been updated.*

Minnesota's first-ever post-election review in November 2006 – a manual count of votes from randomly-selected precincts in the state – drew praise from two sides that do not always see eye-to-eye, election officials and advocacy groups.

"I believe that Minnesota has done a most remarkable job at making every vote count and count correctly," said Janet Straub, a Minnesota resident and observer of the audit.[22]

Secretary of State Mark Ritchie (DFL) said he was also impressed. "I am excited to hear the very positive results from our first reviews. We can all feel a great deal of confidence in our election results - and only hope that other states can catch up to our system before the 2008 elections," he said in a press release from Citizens for Election Integrity Minnesota.[23]

The law mandating the new procedure was spearheaded by state Rep. Bill Hilty, DFL-Finlayson. "We have a really good system in place in Minnesota. We have a 100 percent paper-ballot system. But even with these devices the only way to be confident in their security and reliability is to check them out," Hilty stated.[24]

Depending on the number of registered voters in a county, two to four precincts per jurisdiction must be randomly selected for auditing. Hilty said he hopes to fine tune the law during the current legislative session by requiring more populous counties to audit more precincts.

Presidential, gubernatorial and congressional races are examined. Local election officials and election judges perform the check, hand-counting the paper ballots and comparing them with the optical-scan tabulation results. The comparison is required to be accurate to within one-half of 1 percent and, if it is not, more precincts are reviewed.[25]

In many counties, precincts were selected less than a week after Election Day, with most counties performing reviews within days of the precincts' selection, generally at county courthouses.

The selection of the precincts was open to the public, as was the review. Citizens for Election Integrity Minnesota and the League of Women Voters Minnesota teamed up to organize observers in 70 of the state's 87 counties. The state has over 4,100 precincts of which a about 200 were reviewed.[26]

"Based on reports from our observers in 70 counties, we are impressed by the accuracy of the machines that were reviewed and the professionalism of the county election officials," Mark Halvorson, director of Citizens for Election Integrity Minnesota, stated in a press release.[27]

Some county election officials, however, were initially skeptical of the new requirement, including Kevin Corbid, Washington County's election director.

"When the post-election audit was passed in Minnesota, I frankly was not a big proponent. Any local election official understands the enormous amount of work that is done by county auditors, county election staff, city and township staff and election judges. The idea of adding more duties was not appealing," Corbid stated.[28]

He added the proper testing of the equipment before an election goes a long way to ensuring a secure and reliable vote.

The county has more than 150,000 registered voters and 87 precincts. It took just under five hours to complete the review of four precincts. Of the 12 races reviewed, seven had exact matches; four races saw one vote added each to a candidate and one race saw two votes added to a candidate.

Corbid said the discrepancies were not the result of machine error but rather how the ballots had been marked. In some cases ballots either had check marks or an "X" marked outside the oval or voters had circled the candidate's name, which could not be picked up by the optical-scan machine but was found during the manual count.

Ultimately, despite his initial concerns, he was satisfied with the review.

"I was surprised at how quickly the audit went. I was not surprised by the quality performance of the equipment and our election judges…if this is what is needed to provide some assurance to those who do not have as much confidence in the system then I have no problem continuing to do the audits," he stated.[29]

Anoka County, with more than 180,000 registered voters and 123 precincts, also reviewed four precincts. The process was observed by 20 people and took approximately three hours to conclude. Rachel Smith, Anoka County elections supervisor, deemed the day a success.

"I was very happy with the outcome. It was smooth and efficient," she said. "Any way we can be proactive and people know their vote is being counted is a good thing."[30]

Nevada and Arizona: Challenges in Auditing

In 2004, Nevada was a trailblazer not only for the statewide use of electronic voting machines with voter-verified paper audit trails (VVPATs) but also for the decision by election officials to conduct a post-election audit of paper records to test the accuracy of voting systems.

All 17 Nevada counties conducted audits after the primary and general elections and all showed no variation between the machine records and the VVPATs.[31] County clerks or registrars were required to audit four machines or 3 percent of machines, whichever number is greater, in counties with populations of 100,000 or fewer, 20 machines or 2 percent of machines, whichever number is greater, in counties with populations more than 100,000, resulting in an audit of 145 machines statewide after the general election. According to a press release from the secretary of state's office, not a single vote changed.[32]

However, counties used different audit methods. Officials in Clark County, the state's most populous county and home to Las Vegas, compared tallies from hand-counted VVPATs with electronic results while other counties compared VVPAT totals to tallies logged by machines' internal counters.

Some counties began to consider using hand-held scanners to read barcodes printed on the VVPAT to hasten the process.

Larry Lomax, Clark County voter registrar explained that the "tedious" audit process took as long as four minutes per VVPAT. Mistakes, he said, were common.

"Our biggest problem was human error. Manual auditing is a boring, tedious process that takes a long time even if done without error. If one person makes one mistake on a tape, then it has to be re-audited. That occurred about a third of the time in our first attempt at manual auditing," Lomax said.[33]

Meanwhile, paper-trail advocates shared concerns about using scanners for audits. "The purpose of an audit is to have an independent check. If bar-code readers are supplied by the same vendor as the rest of the voting system, it's not an independent check...Reading bar codes is not 'manual auditing' in my book," said David Dill, founder of *VerifiedVoting.org*.

Dan Burk, Washoe County voter registrar, said that the scanners would not be purchased from Sequoia, the voting machine vendor, and would be publicly tested before use in an audit.[34]

State administrative code was changed in July 2006 to allow for the use of scanners or hand counts saying that audits "may be conducted manually or by a mechanical device" approved by the Secretary of State.[35]

After using hand-held scanners to audit the 2006 general election, Lomax said he was pleased with their performance. "It worked great, it definitely cuts the time down astronomically and we don't have to deal with the same problem of human error ..... this worked much better for us," he said. However, scanners may not be necessary for all counties as some have less than 1,000 voters in a given election.[36]

Lomax said that he has had conversations with an individual working for the National Institute for Standards and Technology regarding the scanners because the voters have only confirmed their votes on the ballot and not the bar-code that gets printed on it. However, Clark County uses open-source code to program the scanners and Lomax emphasized that voters are comfortable with electronic voting machines because they have been using them for more than 10 years.[37]

Arizona: Seeking to Close an Audit Loophole

Arizona requires post-election audits, but with a catch.

An audit can only be performed if people show up to do it. If not, the audit is not required. And that has made post-election verification relatively rare in the state. Only five of the state's 15 counties – Gila, Maricopa, Mohave, Pima and Yuma – performed manual audits following the 2006 general election.[38]

"Right now, two parties have to show up to do an audit...and that's not right," John Brakey of Americans United for Democracy, Integrity and Transparency in Elections – Arizona said. "If one party shows up and the other one isn't there, it's cancelled."[39]

The state's current audit rules started with the intention to perform a more thorough count. In January 2006, a bipartisan group of lawmakers introduced S.B. 1557, legislation that would have required a post-election hand count of ballots from 5 percent of precincts.[40]

Arizona Citizens for Election Reform (ACER) supported the bill

and encouraged citizens to attend related hearings.

"With increasing concern about the security of our voting machines and their effectiveness, Arizona citizens demand that our right to vote be secured and results verified. Problems with electronic voting systems have engendered a loss of public confidence in elections and prompted lawsuits which have been costly both to candidates and to taxpayers," ACER said in a February 2006 press release prior to the hearing. [41]

Following that hearing, the advocacy group VoteTrustUSA reported that the state's Senate Judiciary Committee gutted the bill, "substituting in its place a watered-down version that rendered the bill's effort to restore confidence in Arizona's election meaningless."[42]

The state Senate changed the time frame for a manual audit from seven days after all ballots have been counted to no more than 60 days after the general election.[43] The amended version of S.B. 1557 was signed by Gov. Janet Napolitano (D) in June 2006.[44]

According to the final version, county chairs from the various political parties on the ballot must name at least three registered voters to serve as election board workers per precinct to be audited. If the board workers fail to appear and perform the hand count, the electronic tabulation is deemed the official count.[45]

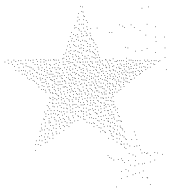
A bill (S.B. 1623) introduced in early 2007 by state Sen. Karen Johnson, R-Mesa, would require the county elections officer to conduct a hand count regardless of whether board workers appear.[46] The measure cleared a Senate committee in February.[47]

"The audit makes me feel better... Based on the audit that we did, I would say 'yes,' [the election was fair]."

-- Tom Ryan, Arizona Citizens for Fair Elections

Pima County's manual audit following the 2006 general election validated that the election's results were within legal limits. Out of more than 15,000 ballots, the hand tally differed from the electronic tally by 47 ballots.

Brad Nelson, director of county elections, explained that the ballot counts may have not matched completely because the machines only counted ballots that were cast correctly while manual auditors counted other marks. Tom Ryan of Arizona Citizens for Fair Elections said, "The audit makes me feel better... Based on the audit that we did, I would say 'yes,' [the election was fair]."[48]



Connecticut: Comprehensive Audits Could Expand

For more than 80 years, Connecticut election officials administered the vote on lever machines, clunky metal contraptions that while capable of producing a satisfying *ker-chunk* when the voter pulls the red bar to cast the ballot, are nonetheless incapable of allowing for a post-election audit of results. The paperless system works mechanically, using internal counters that track each vote as it is cast.

So when the state took its first steps toward replacing the lever machines by adopting a pilot project to use optical-scan systems in 25 jurisdictions statewide, a comprehensive audit program was introduced as well. After the November 2006 election concluded, ballots cast in 20 percent of precincts in jurisdictions covered by the pilot project were hand counted and compared to the totals produced by electronic counts under a project devised by the University of Connecticut's Department of Computer Sciences and the Secretary of State's office.[49]

Perfect match

The pilot project involved performing a hand count of every voting machine used in 17 precincts within the 20 towns in the pilot project. In most cases, auditors found the results "matched up perfectly." When they did not, mis-marked ballots, including those with stray marks that rendered them uncountable by machines, were the culprit.[50]

Secretary of State Susan Bysiewicz (D) said that the decision to audit such a high percentage of machines when compared with audits performed in other states was the result of discussions between her office, university researchers and groups that included the League of Women Voters and TrueVoteCT, a nonpartisan organization that promotes "accessible and verifiable voting."[51]

"We think it's important to get a significant sample because you want people in Connecticut to be confident that our voting machines are secure and accurate," Bysiewicz said. "We had the closest congressional race in the country where [Rep. Joe Courtney, D-Conn.] won by 83 votes. Ten of 65 towns used new voting machines and in those 10 towns there were no discrepancies in the post-election audit."[52]

Mary Mourey, Republican registrar of voters for East Hartford, oversaw one of the largest such post-election audits in the state in 2006. Her jurisdiction had three precincts to audit following the vote. Using teams of two counters -- one Democrat and one Republican -- more than 5,000 ballots were tallied in a single day three weeks after Election Day.

"We were very pleased, the first time doing something like this," she said. "It was a perfect match."[53]

While she said auditing the results of the previous election did not present an unreasonable demand, a high-turnout presidential vote could prove more onerous.

Audit rules pending

But that could be the future in the Nutmeg State. After the successful post-election audit of the pilot program in 2006, Bysiewicz introduced legislation in 2007 that would make 20 percent audits a fixture of Connecticut elections as optical-scan voting systems are implemented statewide.

The legislation would require the completion of a manual audit of 20 percent of precincts two days before the canvass for any federal or state election. Similar to the pilot program, precincts would be randomly selected for auditing.[54]

While Bysiewicz acknowledged the 20 percent figure represented a potentially large pool of ballots, she said it was a worthwhile endeavor.

"We understand that there are other pieces of legislation pending in Congress and in other states that would have a much smaller requirement, but we decided to go with the 20 percent because that's what we did for the audit for the first 20 towns," she said. "We think it's important to get a significant sample because you want people in Connecticut to be confident that our voting machines are secure and accurate."

"There may be some who say that's too much work, but I would argue the voter confidence is very important, particularly in the first year we use these machines," she added.[55]

Some advocates have raised issue with the broad discretion afforded to the Secretary of State in the event of a discrepancy discovered during auditing, as well as the timetable for conducting the post-election counts, arguing it would be too late for candidates to act on information gleaned from the process.

SNAPSHOT OF THE STATES: Audit Requirements

The following states require a post-election manual audit of ballots, a post-election mechanical audit of ballots, a post-election audit of election records and/or a post-election audit of voting systems. States without audit rules were not included.

Alaska

Audit type: Hand ballot count

Who conducts review: Local election official with the assistance of appointed representatives from the political parties.[56]

Timing: Begins as soon as practicable after the election but no later than 16 days after an election.[57]

Audit scope: One randomly selected precinct in each election district that accounts for at least 5 percent of the ballots cast in that district.[58]

Remedy for potential discrepancies: If there is a discrepancy of more than 1 percent between the results of the hand count and the certified count, the director will conduct a hand count of the ballots from that district. If there is an unexplained discrepancy in the ballot count in any precinct, the director may count [additional] ballots from that precinct.[59]

Arizona

Audit type: Hand ballot count

Who conducts review: The county election officer and county political party chairs or person designated conduct the selection of precincts. The county party chairs designate at least three board workers to perform the hand count. If the board workers fail to appear, no hand count is conducted.[60]

Timing: Precinct selection begins after all ballots have been delivered to the central counting center. The unofficial vote totals from all precincts are made public before selecting the precincts to be hand counted.[61] Hand counts begin within 24 hours after the closing of the polls and are completed before the canvassing of the election.[62]

Audit scope: At least 2 percent of the precincts in the county, or two precincts, whichever is greater. At least four contested races, including one federal race, one statewide candidate race, one ballot measure and one legislative race on those ballots shall be counted. During presidential elections, the presidential race is also counted.[63]

Remedy for potential discrepancies: If there are discrepancies between the two counts greater than the designated margin, a second hand count is performed. If the second hand count still has a difference greater than the designated margin, the hand count is expanded to include a total of twice the original number of randomly selected precincts.[64]

California

Audit type: Hand ballot count

Who conducts review: Local election official[65]

Timing: Conducted during the official canvass.[66] The process is open to the public.[67]

Audit scope: At least 1 percent of randomly selected precincts. If 1 percent of the precincts is less than one whole precinct, the count will be conducted in one precinct chosen at random by the elections official. For each race not included in the initial group of precincts, one additional precinct will be counted. Additional precincts are selected at the discretion of the election official.[68]

Remedy for potential discrepancies: A report on the results will identify discrepancies between the machine count and the manual tally and describe how the discrepancies were resolved. The VVPAT governs if there is a discrepancy between it and the electronic record.[69]

Colorado

Audit type: Hand ballot count

Who conducts review: The Secretary of State initiates the manual random audit to be conducted by each county.[70] The audit is observed by at least two members of the canvass board of the county.[71]

The designated election official can appoint additional deputized clerks to assist.[72]

Timing: Within 24 hours of polls closing, the Secretary of State notifies election officials which voting devices and which races have been selected for auditing.[73]

Audit scope: A random selection of 5 percent of precinct scanner-based equipment, at least one central count scanner/vote center and 5 percent of direct-recording electronic (DRE) voting systems.[74]

Remedy for potential discrepancies: If there is any discrepancy which cannot be accounted for by voter error, the county clerk and recorder investigates and takes such remedial action as necessary.[75]

Connecticut[76]

Audit type: Hand ballot count[77]

Who conducts review: The 2006 audit was performed by the Office of the Secretary of State with the assistance of the University of Connecticut's Department of Computer Sciences. Officials from the League of Women Voters randomly chose the precincts.[78]

Timing: The audit was performed during the final week of November.[79]

Audit scope: Ballots were reviewed in 17 precincts, representing 20 percent of the 87 polling precincts in the 15 cities and towns which used optical-scan technology in the 1st, 3rd, 4th, and 5th Congressional districts.[80]

Remedy for potential discrepancies: In the majority of the precincts, the counts matched and in those where the results did not match, there were only minor changes reported. In each instance, the change was due to a mismarked ballot, not to machine error.[81]

Florida

Audit type: Non-mandatory audit of voting system, including checks against "unauthorized manipulation and fraud."

Timing: At any time the Department of State can review the voting system of any county to ensure compliance with the Electronic Voting Systems Act.[82]
If directed, the legislature can also provide for an independent audit of a voting system in any county. It shall consist of a study and evaluation of the voting system and provide reasonable assurance that the system is properly controlled, can accurately count votes, provides adequate safeguards against unauthorized manipulation and fraud, and complies with the requirements of law and rules of the Department of State.[83]

Hawai'i

Audit type: Hand ballot count

Who conducts review: The local chief election officer[84]

Timing:Prior to certification of election results.[85]

Audit scope: A random sample of not less than 10 percent of the precincts employing the electronic voting system.[86]

Remedy for potential discrepancies: If discrepancies appear, the chief election officer immediately conducts an expanded audit to determine the extent of misreporting in the system.[87]

Illinois

Audit type: Hand ballot count

Who conducts review: The local chief election officer. The state central committee chair of each party can be represented at the procedure.[88]

Timing: After Election Day and before election results are declared.[89]

Audit scope: 5 percent of precincts.[90]

Remedy for potential discrepancies: The election authority immediately forwards a written report to the appropriate canvassing board explaining the results of the test and any errors encountered and the report shall be made available for public inspection.[91]

Kentucky

Audit type: Hand ballot count

Who conducts review: The state board of elections prescribes rules and regulations.[92]

Timing: As part of the official canvass.[93]

Audit scope: Random selection of between 3 and 5 percent of total ballots cast.[94]

Remedy for potential discrepancies: Not specified

Maryland

Audit type: Election records, including signed voter authority cards, precinct registers, other polling place forms completed by the election judges and the official election results.

Who conducts review: Local boards of election.

Audit scope: Vote totals are verified by comparing printed forms from individual voting units to reports generated by the central tabulator.

Remedy for potential discrepancies: The local board continues its audit until it determines the cause of the discrepancy.[95]

Minnesota

Audit type: Hand ballot count

Who conducts review: The county canvassing board appoints a post-election review official who can be assisted by election judges. The review is conducted in public.[96]

Timing: At the canvass of the state primary, the county canvassing board sets the date, time and place for the post-election review of the general election. At the canvass of the state general election, county canvassing boards select the precincts to be reviewed.[97]

Audit scope: Counties with fewer than 50,000 registered voters must review at least two precincts. Counties with between 50,000 and 100,000 registered voters must review at least three precincts. Counties with over 100,000 registered voters must review at least four precincts. At least one precinct selected in each county must have had more than 150 votes cast at the general election.[98] The post-election review must be conducted of the votes cast for President or Governor; U.S. Senator; and U.S. Representative.[99]

Remedy for potential discrepancies: If the review reveals a difference greater than one-half of 1 percent, within two days there will be an additional review of at least three precincts. If the second review also shows a difference greater than one-half of 1 percent, a review of the ballots from all the remaining precincts in the county must be performed. If the results from the county reviews from one or more counties comprising more than 10 percent of the total number of persons voting indicate an error in counting has occurred, a manual recount of all ballots in the district for the affected office must be performed.[100]

Missouri

Audit type: Hand ballot count

Who conducts review: The county election authority selects at least one team made up of at least two members.[101]

Timing: After the mandated electronic recount and prior to the certification of election results.[102]

Audit Scope: At least one precinct for every 100 election precincts. One contested race is selected from the following categories: President, U.S. Senate and statewide candidates; statewide ballot issues; U.S. Representative candidates and state General Assembly candidates; partisan circuit and associate circuit judge candidates and all nonpartisan judicial retention candidates; and in addition not less than three contested races or ballot issues from all political subdivisions and special districts, including the county, in the selected precinct(s). When there are three or fewer contested races or ballot issues within this category at a selected precinct, all must be counted.[103]

Remedy for potential discrepancies: Not specified

Nevada

Audit type: Hand ballot count or mechanical audit (including bar-code scanners for voter-verified paper audit trails).

Who conducts review: County clerk.[104] The public can observe.[105]

Timing: The results of the audit must be sent to the Secretary of State within seven working days after the election.[106]

Audit scope: Counties whose population is 100,000 or more must audit 2 percent of voting machines used in the election or no less than 20 voting machines, whichever is greater. Counties whose population is less than 100,000 must audit 3 percent of voting machines used in the election or no less than four voting machines, whichever is greater.[107] The comparison may be conducted manually or by a mechanical device determined by the Secretary of State to be capable of accurately reading the votes cast.[108]

Remedy for potential discrepancies: Not specified.

New Mexico

Audit type: Hand ballot count

Who conducts review: The Secretary of State directs county clerks. Canvass observers are allowed.[109]

Timing: Within five days of the completion of the county canvass.[110]

Audit scope: For votes in the general election for the office of President or Governor, 2 percent of the voting systems in the state are compared with votes tallied by hand from the voter-verifiable and auditable paper trail from those voting systems.[111]

Remedy for potential discrepancies: For voting machines not used for absentee voting, if totals differ by more than 1.5 percent, a recount is conducted for the office in the precincts of the legislative district where the discrepancy occurred.[112]

New York

Audit type: Hand ballot count

Who conducts review: The board of elections or a bipartisan committee appointed by the board.[113]

Timing: Within 15 days after each general or special election and within seven days after every primary or village election conducted by the board of elections.[114]

Audit scope: At least 3 percent of voting systems within the jurisdiction.[115]

Remedy for potential discrepancies: Standards created by the Board of Elections will determine when a discrepancy between the manual audit tallies and the voting system tallies requires an audit of additional voting systems. [116] Any board of elections shall be empowered to order any such audit to be conducted whenever such discrepancy exists.[117]

North Carolina

Audit type: Hand ballot count

Who conducts review: The State Board of Elections creates the procedure for randomly selecting the precincts for each election.[118]

Timing: The selection of precincts is done after the initial count of election returns is publicly released or 24 hours after the polls close on Election Day, whichever is earlier.[119]

Audit scope: The sample chosen by the state board is of one or more full precincts, full counts of mailed absentee ballots, full counts of one or more one-stop early voting sites, or a combination. The size of the sample of each category is chosen to produce a statistically significant result in consultation with a statistician.[120]

Remedy for potential discrepancies: If the discrepancy between the manual count and the mechanical or electronic count is significant, a complete manual count is conducted.[121]

Oregon:

Audit type: Audit of voting system. Not mandatory. Any voting machine or vote tally system involving the use of computers, a computer network, computer program, computer software or computer system is subject to audit by the Secretary of State at any time for the purpose of checking the system's accuracy.[122]

Pennsylvania

Audit type: Not specified

Who conducts review: County boards of election[123]

Timing: As part of the canvass of returns.[124]

Audit scope: A statistical recount of a random sample of ballots after each election. The sample shall include at least 2 percent of the votes cast or 2,000 votes, whichever is lesser.[125]

Remedy for potential discrepancies: Not specified

Texas

Audit type: Hand count of ballot images

Who conducts review: The general custodian of election records who conducts an election in which a DRE is used for the first time. Candidates are entitled to be present and have a representative present. The designated election official can appoint additional deputized clerks to assist.[126]

Timing: The manual count begins within 72 hours after the close of polls.[127]

Audit scope: A manual count in 1 percent of the election precincts or three election precincts, whichever is greater. For DRE devices the appropriate official will print the cast vote records (ballot images) and manually count the race assigned and verify the manual count matches the election results.[128]

Remedy for potential discrepancies: If there are discrepancies, the election official continues the audit until it determines the cause of the discrepancy. If the discrepancy can not be resolved, the Secretary of State's office is notified.[129]

Utah

Audit type: Hand ballot count

Who conducts review: Local election officials[130]

Timing: After polls close on Election Day but no later than noon the next day, the Lieutenant Governor's (chief election officer) office notifies the appropriate election officers which voting machines will be audited. The machines are audited between the closing of polls and the meeting of the jurisdictions' board of canvassers.[131]

Audit scope: 1 percent of the total number of AccuVote TSx and precinct count AccuVote OS voting machines in use statewide.[132]

Remedy for potential discrepancies: The reasons for any differences between the hand count and the machine total report results are recorded in a log.[133]

Washington

Audit type: Hand ballot count required for some, not all, of ballots selected for review

Who conducts review: County auditor. Political party representatives must be allowed to observe if representatives have been appointed and are present at the time of the audit.[134]

Timing: Prior to certification of the election.[135]

Audit scope: Random selection of up to 4 percent of the DRE devices or one DRE device, whichever is greater. On one-fourth of the devices, the paper records must be tabulated manually. For the remaining devices, the paper records may be tabulated by a mechanical device determined by the secretary of state to be capable of accurately reading the votes cast and printed.[136]

Remedy for potential discrepancies: The paper record produced must be stored and maintained for use in the random audit of results. When such paper record is for an audit it shall be the official record of the election.[137]

West Virginia

Audit type: Hand ballot count

Who conducts review: Board of canvassers[138]

Timing: During the canvass.[139]

Audit scope: At least 5 percent of the precincts chosen at random will have the VVPATs counted manually.[140]

Remedy for potential discrepancies: If the manual count differs by more than 1 percent from the automated tabulation equipment results or there is a different prevailing candidate or outcome of a ballot issue, the discrepancies are disclosed to the public and all VVPATs are manually counted.[141]

Wisconsin

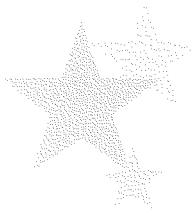
Audit type: Hand ballot count

Who conducts review: The audit consists of two independent processes: an audit conducted by municipalities of reporting units randomly selected by the State Elections Board (SEB) and an audit of reporting units conducted by the SEB. The audit is open to the public.[142]

Timing: Audits are only conducted after the November general election. Officials are notified the day after the election of the voting systems selected for the audit. The audit must be conducted no later than two weeks after the county board of canvassers certifies the election results.[143]

Audit scope: The SEB will randomly select 50 reporting units across the state, including a minimum of five reporting units for each voting system used in the state. A minimum of four contests are audited, including the top candidate race on the ballot. The other contests are selected randomly but must appear on every ballot in the state. The SEB may also audit additional contests.[144]

Remedy for potential discrepancies: If the hand counts and vote tallies do not match, the results are double-checked. If they still do not match, the difference is noted on the appropriate form. The SEB will request the vendor investigate and explain the reasons for any differences between the machine tally and the paper record tally. If the vendor fails to provide a sufficient explanation the SEB will suspend approval of all voting systems manufactured or serviced by the vendor.[145]



Methodology/Endnotes

Research was compiled through the use of primary and secondary sources, including interviews with state and local election officials, data derived from state law, state election division Web sites, news accounts and information provided by other non-governmental organizations.

All sources are cited below in the endnotes.

The opinions expressed by election officials, lawmakers and other interested parties in this document do not reflect the views of nonpartisan, non-advocacy electionline.org or the Election Reform Information Project.

All questions concerning research should be directed to Sean Greene, research director, at *sgreene@electionline.org*.

1 Feinstein, the Hon. Dianne. "Statement of Chairman Feinstein at Rules Committee Hearing to Evaluate Electronic Voting Systems," Feb. 7, 2007, *http://feinstein.senate.gov/07releases/r-rules-hearing0207.htm*.

2 Norden, Lawrence. "The Machinery of Democracy: Voting System Security, Accessibility, Usability and Cost," The Brennan Center for Justice, 2006.

3 "Verified Voting Applauds League of Women Voters Passage of Resolution in Support of Voter-Verified Paper Records, Audits," *VerifiedVoting.org*, June 12, 2006.

4 "Voting is cast for ballot audit trail," *The Atlanta Journal-Constitution*, June 16, 2005.

5 For other detailed research about post-election manual audits, please see "Manual Audit Requirements," Verified Voting Foundation, November 2006, *www.verifiedvoting.org/downloads/StateManualAuditProvisions-11-06.pdf* (last visited Feb. 14, 2007).

6 For more information, see California section on page 7.

7 "Voting System Audit Requirements," Wisconsin State Elections Board, November, 2006, *http://elections.state.wi.us/docview.asp?docid=9851&locid=47* (last visited Feb. 12, 2007).

8 Tokaji, Dan. "Convictions in Ohio Recount Tampering Case," *Equal Vote Blog*, Jan. 25, 2007, *http://moritzlaw.osu.edu/blogs/tokaji/2007/01/convictions-in-ohio-recount-tampering.html* (last visited Feb. 20, 2007).

9 Kropko, M. R. "Prosecutor says presidential recount rigged in Ohio county," *The Associated Press* as published in *The Beacon Journal*, Jan. 18, 2007.

10 Gibson, Bob. "Voting machine changes advance," *The Daily Progress*, Feb. 13, 2007

11 Kentucky Statutes § 117.383(8).

12 Maryland State Board of Elections Web site, *www.elections.state.md.us/voting_system/testing.html* (last visited Feb. 12, 2007).

13 Wallach, Dan S. "Testimony of Dan S. Wallach, Associate Professor of Computer Science, Rice University, Before the Senate Committee on Rules and Administration," Feb. 7, 2007.

14 California Elections Code § 336.5, 15360

15 The California Voter Foundation. "Governor Signs Landmark Bill to Require Public Audits of Software Vote Counts," Press Release, Oct. 11, 2005.

16 Salladay, Robert. "Democracy Gets Audited in California," *Los Angeles Times*, Nov. 29, 2006.

17 *Ibid.*

18 San Mateo County Web site: *www.shapethefuture.org*, posted Nov. 17, 2006.

19 *Ibid.*

20 Gordon, Rebekah. "Elections Office Gets Tips From Experts," *San Mateo County Times*, Nov. 30, 2006.

21 *Op. Cit.* Salladay.

22 E-mail correspondence with Janet Straub, Dec. 6, 2006.

23 "Results from Minnesota's First Post-Election Review Confirms Accuracy of State's Voting Machines," Press Release: Citizens for Election Integrity Minnesota, Nov. 15, 2006.

24 Phone interview with Rep. Bill Hilty, Dec. 7, 2006.

25 "Post-Election Voting System Review," Office of the Minnesota Secretary of State, September 2006.

26 *Op. cit.* Citizens for Election Integrity.

27 *Ibid.*

28 E-mail correspondence with Kevin Corbid, Washington County clerk, Dec. 5, 2006.

29 *Ibid.*

30 Phone interview with Rachel Smith, Anoka County clerk, Dec. 6, 2006.

31 "Audit: No tabulation problems with new Nevada voting machines," *The Associated Press* as reported on *KRNV.com*, Sept. 27, 2004.

32 Heller, The Hon. Dean. Press release: "State Canvass of 2004 General Election Completed," Office of the Secretary of State of Nevada, Nov. 23, 2004.

33 Greene, Sean. "Nevada Officials Eye Barcodes, Scanners to Speed Paper-Trail Counting," *electionline Weekly*, Feb. 16, 2006.

34 *Ibid.*

35 NAC 293.255.

36 Phone interview with Larry Lomax, Feb. 15, 2007.

37 *Ibid.* Feb.16, 2007.

38 Arizona Secretary of State Jan Brewer, "Hand Count Results – 2006 General Election." *www.azsos.gov/election/2006/general/handcountresults.htm*.

39 Phone interview, Feb. 19, 2007.

40 Arizona State Senate, 47th Legislature, 2nd Regular Session, 2006. SB 1557. *www.azleg.gov/FormatDocument.asp?inDoc=/legtext/47leg/2r/bills/sb1557p.htm*.

41 Arizona Citizens for Election Reform, "Call for Citizen Support of SB 1557," Feb. 13, 2006.

42 Stewart, Warren. "Arizona: State Senator Huppenthal Guts Election Reform Bill," VoteTrust USA, Feb. 15, 2006.

43 Arizona State Legislature, 47th Legislature, 2nd Regular Session, 2006. Committee on Judiciary, Senate amendments to SB 1557.

44 Arizona State Legislature, 47th Legislature, 2nd Regular Session, 2006. Bill status overview, SB 1557.

45 Arizona State Senate, 47th Legislature, 2nd Regular Session, 2006. Chapter 394, SB 1557.

46 Arizona State Senate, 48th Legislature, 1st Regular Session, 2007. Fact sheet for SB 1623.

47 Arizona State Legislature 48th Legislature, 1st Regular Session, 2007. SB 1623 bill status overview.

48 Rathbun, Sandy. "Audit confirms Pima County election results," KVOA Tucson News 4, Nov. 14, 2006.

49 Bysiewicz, The Hon. Susan. Press release: "Audit Report Shows Optical Scan Machines Performed Very Well in 2006 Elections," Office of the Secretary of State of Connecticut, Dec. 7, 2006.

50 *Ibid.*

51 From "About Us," *TrueVoteCT.org*, last visited Feb. 15, 2007.

52 Phone interview with Connecticut Secretary of State Susan Bysiewicz, Feb. 8, 2007.

53 Phone interview with Mary Mourey, East Hartford registrar of voters, Feb. 15, 2007.

54 Connecticut General Assembly

55 *Op. Cit.*, Bysiewicz.

56 Alaska Statutes § 15.15.420.

57 Alaska Statutes § 15.15.440.

58 Alaska Statutes § 15.15.430.

59 *Ibid.*

60 Arizona Revised Statutes § 16-602(C).

61 *Ibid.*

62 Arizona Revised Statutes § 16-602(J).

63 Arizona Revised Statutes § 16-602(C).

64 Arizona Revised Statutes § 16-602(D).

65 California Elections Code § 153609(a).

66 *Ibid.*

67 California Elections Code § 153609(d).

68 California Elections Code § 153609(a).

69 California Elections Code § 153609(e).

70 Colorado Revised Statutes § 1-7-514 (1) (a) (I).

71 Colorado Revised Statutes § 1-7-514 (4).

72 8 CCR 1505-1: 11.5.4.7.

73 8 CCR 1505-1: 11.5.4.1.

74 8 CCR 1505-1: 11.5.4.2.

75 Colorado Revised Statutes § 1-7-514 (2)(a).

76 In 2005, the Connecticut legislature passed a law requiring a manual audit for DRE voting machines with VVPATs. These systems, however, are not in use in the state. The state conducted an audit of 20 percent of optically-scanned ballots after the 2006 general election as part of a pilot program that introduced the system to a limited number of voting jurisdictions. Legislation mandating a similar audit statewide is pending.

77 Bysiewicz, The Hon. Susan. Press release: "Secretary Bysiewicz: Towns Randomly Chosen to have Optical Scan Voting Machines Audited," Office of the Secretary of State of Connecticut, Nov. 15, 2006.

78 Bysiewicz, The Hon. Susan. Press release: "Audit Report Shows Optical Scan Machines Performed Very Well in 2006 Elections," Office of the Secretary of State of Connecticut, Dec. 7, 2006.

79 *Ibid.*

80 Bysiewicz, The Hon. Susan. Press release: "Secretary Bysiewicz: Towns Randomly Chosen to have Optical Scan Voting Machines Audited," Office of the Secretary of State of Connecticut, Nov. 15, 2006.

81 Bysiewicz, The Hon. Susan. Press release: "Audit Report Shows Optical Scan Machines Performed Very Well in 2006 Elections," Office of the Secretary of State of Connecticut, Dec. 7, 2006.

82 Florida Statutes §101.5607.

83 Florida Statutes §101.591.

84 Hawaii Statutes § 16-42(3).

85 *Ibid.*

86 *Ibid.*

87 Hawaii Statutes § 16-42(4).

88 Illinois Statutes Art. 10 § 5/24C-15.

89 *Ibid.*

90 *Ibid.*

91 *Ibid.*

92 Kentucky Statutes § 117.383(8).

93 *Ibid.*

94 *Ibid.*

95 Maryland State Board of Elections Web site, *www.elections.state.md.us/voting_system/testing.html* (last visited Feb. 12, 2007).

96 Minnesota Statutes § 206.89 (Subd. 3).

97 Minnesota Statutes § 206.89 (Subd. 2).

98 *Ibid.*

99 Minnesota Statutes § 206.89 (Subd. 3).

100 Minnesota Statutes § 206.89 (Subd. 5).

101 15 CRS 30-10.110 (2)

102 *Ibid.*

103 15 CRS 30-10.110 (2), (3C)

104 NAC 293.255(1).

105 NAC 293.255(6).

106 NAC 293.255(5).

107 NAC 293.255(3)(4).

108 NAC 293.255(2).

109 New Mexico Statutes § 1-14-13.1(A).

110 *Ibid.*

111 *Ibid.*

112 New Mexico Statutes § 1-14-13.1(B).

113 New York State Consolidated Laws § 9-211(1).

114 *Ibid.*

115 *Ibid.*

116 *Ibid.*

117 New York State Consolidated Laws § 9-211(3).

118 North Carolina General Statutes § 163-182.1(b)(1).

119 *Ibid.*

120 *Ibid.*

121 *Ibid.*

122 Oregon Statutes § 246.565(1).

123 Pennsylvania Statutes § 3031.17.

124 *Ibid.*

125 *Ibid.*

126 McGeehan, Ann. "Election Advisory No. 2006-16," Sept. 13, 2006 *www.sos.state.tx.us/elections/laws/advisory2006-16.shtml* (last visited, Feb. 14, 2007).

127 *Ibid.*

128 *Ibid.*

129 *Ibid.*

130 "Election Policy," State of Utah, Office of the Lieutenant Governor, Oct. 17, 2006.

131 *Ibid.*

132 *Ibid.*

133 *Ibid.*

134 Washington Code § 29A.60.185.

135 *Ibid.*

136 *Ibid.*

137 Washington Code § 29A.60.095.

138 West Virginia Code § 3-4A-28(d).

139 *Ibid.*

140 *Ibid.*

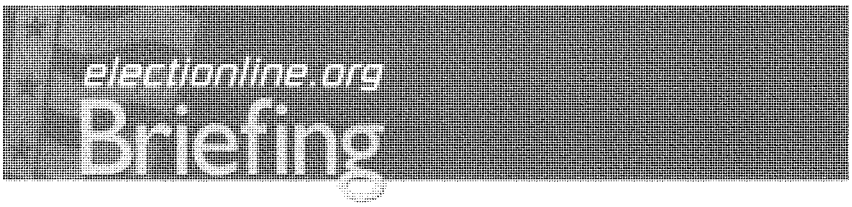
141 West Virginia Code § 3-4A-28(d)(1)(2).

142 "Voting System Audit Requirements," Wisconsin State Elections Board, November, 2006, *http://elections.state.wi.us/docview.asp?docid=9851&locid=47* (last visited Feb. 12, 2007).

143 *Ibid.*

144 *Ibid.*

145 *Ibid.*



electionline.org, administered by the Election Reform Information Project, is the nation's only nonpartisan, non-advocacy website providing up-to-the-minute news and analysis on election reform.

After the November 2000 election brought the shortcomings of the American electoral system to the public's attention, The Pew Charitable Trusts made a grant to the University of Richmond to establish a clearinghouse for election reform information.

Serving everyone with an interest in the issue – policymakers, officials, journalists, scholars and concerned citizens – *electionline.org* provides a centralized source of data and information in the face of decentralized reform efforts.

electionline.org hosts a forum for learning about, discussing and analyzing election reform issues. The Election Reform Information Project also commissions and conducts research on questions of interest to the election reform community and sponsors conferences where policymakers, journalists and other interested parties can gather to share ideas, successes and failures.

electionline.org
Your first stop for election reform information

1025 F Street NW
Suite 900
Washington, DC 20004
tel: 202-552-2000
fax: 202-552-2299
www.electionline.org

Election Reform Information Project

A Project of the University of Richmond
supported by The Pew Charitable Trusts

THE PEW CHARITABLE TRUSTS

Serving the public interest by providing information, policy solutions and support for civic life.

ELECTION REFORM: AUDITING THE VOTE

ELECTION REFORM:
AUDITING THE VOTE