

ELECTRONIC VOTING SYSTEM SECURITY

WEDNESDAY, JULY 7, 2004

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

The committee met, pursuant to call, at 11:00 a.m., in room 1310, Longworth House Office Building, Hon. Robert W. Ney (chairman of the committee) presiding.

Present: Representatives Ney, Ehlers, Mica, Larson, Millender-McDonald, and Brady.

Also Present: Representatives Hoyer and Holt.

Staff Present: Paul Vinovich, Staff Director; Matt Petersen, Counsel; Payam Zakipour, Professional Staff Member; George Shevlin, Minority Staff Director; Charlie Howell, Minority Chief Counsel; Matt Pincus, Minority Professional Staff Member; Catherine Tran, Minority Professional Staff Member; Thomas Hicks, Minority Professional Staff Member; and Kellie Cass-Broussard, Minority Professional Staff Member.

The CHAIRMAN. The committee will come to order. I am going to begin my opening statement. Mr. Larson is on his way and we have Mr. Ehlers. The committee is meeting today to discuss electronic voting system security, an issue that has garnered extensive media attention and produced impassioned opinions on all sides in recent months. Hopefully, this committee hearing will be able to shed some light on a matter that has certainly generated plenty of intense heat across the Nation. After the controversial presidential election of 2000, in which the term "hanging chad" became part of the national lexicon, Congress enacted and President Bush signed the Help America Vote Act, known as HAVA, to help restore the American public's confidence in the Federal electoral process. The goals of HAVA are simple: to ensure that all eligible Americans have an equal opportunity to vote and have their votes counted, to protect against legal votes being cancelled out by illegal votes, basically making it easier to vote and harder to cheat.

To accomplish these objectives, HAVA established new voter rights providing for second-chance voting, provisional ballots and enhanced access for individuals with disabilities; specifies new voting standards, requires each State to implement a computerized statewide voter registration database; and requires each polling place to publicly post certain voting information, such as sample ballots, instructions regarding provisional ballots and polling place hours. To address issues relating to the security of voting technologies, HAVA creates the Technical Guidelines Development Committee (TGDC) chaired by the director of the National Institute

of Standards (NIST) to aid the Election Assistance Commission in crafting standards and guidelines to ensure the integrity of computer technology being used in current voting systems. Furthermore, HAVA provides for the testing and certification of voting system hardware and software in accredited laboratories.

Following HAVA's passage, many jurisdictions began making plans to replace outmoded voting machines with the latest and most technologically advanced electronic voting equipment. These direct recording electronic (DRE) voting systems have been widely touted as easier for voters to use, thus resulting in fewer spoiled ballots, and, unlike most other voting systems, are capable of allowing individuals with disabilities to vote in a private and independent manner, sometimes for the first time in their lives.

Not everyone is excited about the prospect of widespread electronic voting, however. Over the last year, several technology specialists, concerned citizens, and media outlets have raised serious concerns about the security of DRE voting systems. These critics contend that DREs contain insufficient safeguards to protect against potential efforts by malicious software programmers or computer hackers to skew the results of an election. Moreover, the critics argue that DRE malfunctions or technical glitches could result in scores of votes being lost without any possibility of retrieval.

To address concerns surrounding the security of electronic voting, a number of different bills have been introduced this Congress that would require DRE voting systems to produce a voter verified paper record—a paper receipt listing the choices made by the voter. I have not supported any legislative proposal as of today that would amend HAVA to require DREs to produce paper receipts. As I expressed in a Dear Colleague letter co-signed by my friend Congressman Steny Hoyer and by Senators Mitch McConnell and Christopher Dodd, I believe it would be premature to amend HAVA at this time before the new law has been fully implemented. Doing so could undermine the process established by HAVA for the EAC to develop standards and guidelines for voting systems security.

My reservations about amending HAVA to require paper receipts, however, in no way lessens my interest in assuring that DRE voting systems meet the most rigorous security and operational standards. The American people demand and deserve a voting process in which they can have full confidence, and I will do everything in my power to guarantee that they do.

For this reason, the committee has called today's hearing to hear from a wide range of technology specialists and election administrators to learn more about the issues relating to voting system security. Over the course of the hearing, we will gain a greater understanding about the security measures that DRE voting systems currently have in place and whether they are sufficient to protect against hackers and technical malfunctions. In addition, we hope

to learn more about whether voter verified paper trails are necessary to protect the integrity of the voting process or whether there are other alternatives that can be used. So I look forward to hearing from the witnesses and I will yield to our ranking member.
[The statement of Mr. Ney follows:]

Opening Statement of Chairman Bob Ney
House Administration Committee Oversight Hearing
July 7, 2004

The Committee will come to order. The Committee is meeting today to discuss electronic voting system security—an issue that has garnered extensive media attention and produced impassioned opinions on all sides in recent months. Hopefully, this Committee hearing will be able to shed some light on a matter that has certainly generated plenty of intense heat.

After the controversial presidential election of 2000, in which the term “hanging chad” became part of the national lexicon, Congress enacted, and President Bush signed into law, the Help America Vote Act of 2002 (“HAVA”) to help restore the American public’s confidence in the federal electoral process. The goals of HAVA are simple: (1) to ensure that all eligible Americans have an equal opportunity to vote and have their votes counted, and (2) to protect against legal votes being canceled out by illegal votes.

To accomplish these objectives, HAVA establishes new voter rights providing for second-chance voting, provisional ballots, and enhanced access for individuals with disabilities; specifies new voting system standards; requires each state to implement a computerized statewide voter registration database; and requires each polling place to publicly post certain voting information, such as sample ballots, instructions regarding provisional ballots, and polling place hours.

To address issues relating to the security of voting technologies, HAVA creates the Technical Guidelines Development Committee (“TGDC”), chaired by the Director of the National Institute of Standards and Technology (“NIST”), to aid the EAC in crafting standards and guidelines to ensure the integrity of computer technologies being used in current voting systems. Furthermore, HAVA provides for the testing and certification of voting system hardware and software in accredited laboratories.

Following HAVA’s passage, many jurisdictions began making plans to replace outmoded voting machines with the latest and most technologically advanced electronic voting equipment. These Direct Recording Electronic (“DRE”) voting systems have been widely touted as easier for voters to use, thus resulting in fewer spoiled ballots, and, unlike most other voting systems, are capable of allowing individuals with disabilities to vote in a private and independent manner.

Not everyone is excited about the prospect of widespread electronic voting, however. Over the last year, several technology specialists, concerned citizens, and media outlets have raised serious concerns about the security of DRE voting systems. These critics contend that DREs contain insufficient safeguards to protect against potential efforts by malicious software programmers or computer hackers to skew the

results of an election. Moreover, these critics argue that DRE malfunctions or technical glitches could result in scores of votes being lost without any possibility of retrieval.

To address concerns surrounding the security of electronic voting, a number of different bills have been introduced this Congress that would require DRE voting systems to produce a “voter verified paper record”—a paper receipt listing the choices made by a voter. I have not supported any legislative proposal that would amend HAVA to require DREs to produce paper receipts. As I expressed in a “Dear Colleague” letter co-signed by my friend Congressman Steny Hoyer and by Senators Mitch McConnell and Christopher Dodd, I believe it would be premature to amend HAVA before the new law has even been fully implemented and, consequently, undermine the process established by HAVA for the EAC to develop standards and guidelines for voting system security.

My reservations about amending HAVA to require paper receipts, however, in no way lessen my interest in ensuring that DRE voting systems meet the most rigorous security and operational standards. The American people demand and deserve a voting process in which they can have full confidence, and I will do everything in my power to guarantee that they do.

For this reason, the Committee has called today’s hearing to hear from a wide range of technology specialists and election administrators to learn more about the issues relating to voting system security. Over the course of the hearing, hopefully we will gain a greater understanding about the security measures that DRE voting systems currently have in place and whether they are sufficient to protect against hackers and technical malfunctions. In addition, we hope to learn more about whether voter-verified paper trails are really necessary to protect the integrity of the voting process, or whether there are other alternatives that would be more effective at maintaining DRE voting system security.

We are fortunate to have with us today a number of distinguished individuals, who I will introduce shortly, and who will share with us their knowledge and views about electronic voting system security, and we look forward to hearing from them.

Mr. LARSON. Thank you, Mr. Chairman. I would like to thank you for calling this second of two hearings on a very important topic of elections. The 2000 presidential elections brought to light many problems with the elections process. We heard reports of wide range of voting frustrations, most common were punch cards with hanging and pregnant chads and voters who were turned away from the polls without being given the opportunity to cast a ballot.

This committee has worked tirelessly to enact the Help America Vote Act as a solution to these and other election concerns. As a result of HAVA, \$650 million was provided to the States to replace lever and punch card machines for more modern voting equipment. HAVA does not mandate the type of voting equipment a jurisdiction must use. The decision is left to the States. A few States have opted to require, as the chairman has pointed out, direct recording electronic machines to replace lever and punch card voting equipment. DREs have been in use for elections for over 20 years. According to the 2001 MIT Cal Tech study, DRE machines have a lower residual rate than punch card, lever and optical scan machines. DREs are also fully accessible to disabled voters and they can be modified to the language of voters who may not be proficient in English. An increase ballot font-sized component of the machines can assist voters with vision difficulties as well.

Although some view DRE machines as a panacea for Election Day problems, several computer scientists and advocates have called for a return to paper ballots. I am interested in hearing the witnesses' thoughts on the practicality of implementing a paper trail, and if they believe there is a security problem with DRE machines; and if so, is a paper trail the best answer.

In addition, I would like them to discuss if human factors are being addressed within DRE machines. Is the answer to most of these perceived problems better training for poll workers? I read about the unplugged machines and inadequate training for the process involved in restarting the machinery. But the bigger issue to explore is if electronic voting system security is the most significant problem facing this election or is there a more pressing issue facing us in this election. The MIT Cal Tech study also stated that difficulties with registration were the number one problem with the 2000 elections.

Between 1.5 and 3 million voters were turned away from the polls without casting a ballot on Election Day 2000. I would like the second panel of today's witnesses to highlight the steps that are being taken to ensure that all aspects of HAVA are being followed in order for the American people to have the best election possible this November. My concern is that all of the attention that is being given to voting security will inadvertently suppress voters coming to the polls if they feel their votes will not count; what steps election officials are taking to fix registration problems; will they have enough provisional ballots for the voters.

Two-thirds of the public will vote on the same type of equipment they used in the year 2000. I would like the second panel to review what is being done to ensure that all the voting equipment is secure; what steps are being taken to inform the public that DRE machines are counting ballots correctly. I am also interested in

hearing the witnesses' assessment of the New York Times' editorials calling into question the views and actions of the Senior Senator from Connecticut and one of the chief authors, Chris Dodd and Jim Dickson, the Vice President of Governmental Affairs for the American Association of People with Disabilities who are trying diligently to improve the election process.

Mr. Chairman, I want to thank you and also note that we have two distinguished colleagues joining us today, both the co-author with you of the HAVA bill here in the House, my distinguished leader Steny Hoyer, and probably one of the most knowledgeable people in the House, and I dare say the country, with respect to the issue of electronic voting and paper ballots, Rush Holt, a scientist and physicist, as Mr. Ehlert likes to point out, and a five-time jeopardy winner as well.

So we are graced by their presence and I thank the panelists as well because this is such an important and critical issue to each and every one of us here today.

[The statement of Mr. Larson follows:]

**CHA Oversight Hearing on
Electronic Voting System Security**

July 7, 2004

**11:00 AM
1310 Longworth House Office Building**

REP. JOHN B. LARSON'S OPENING STATEMENT

I would like to thank the Chairman for calling this second of two hearings on the very important topic of elections. The 2000 Presidential election brought to light many problems with the elections process. We heard reports of a wide range of voting frustrations. Most common were punch cards with hanging and pregnant chads, and voters who were turned away from the polls without being given the opportunity to cast a ballot.

This committee worked tirelessly to enact the Help America Vote Act (HAVA) as a solution to these and other election concerns. As a result of HAVA, \$650 million was provided to states to replace lever and punch card machines for more modern voting equipment.

HAVA does not mandate the type of voting equipment a jurisdiction must use. That decision is left to the states. A few states have opted to acquire Direct Recording Electronic (DRE) machines to replace lever and punch card voting equipment. DREs have been used in elections for over 20 years. According to a 2001 MIT/Cal Tech study, DRE machines have a lower residual rate than punch card, lever, and optical scan machines.

DREs are also fully accessible to disabled voters, and they can be modified to the language of voters who may not be proficient in English. An increased ballot font size component on the machine can assist voters with vision difficulties.

Although some view DRE machines as a panacea for Election Day problems, several computer scientists and advocates have called for a return to paper ballots.

I am interested in hearing the witnesses' thoughts on the practicality of implementing a paper trail, and if they believe there is a security problem with DRE machines, is paper the best answer?

In addition, I'd like them to discuss if human factors are being addressed with DRE machines. Is the answer to most of these perceived problems better training for poll

workers? I have read about unplugged machines and inadequate training for process involved in re-starting the machinery.

But a bigger issue to explore is if electronic voting system security is the most significant problem facing this election or is there a more pressing issue facing us this election? The MIT/Cal Tech study also stated that difficulties with registration were the number one problem with the 2000 election. Between 1.5 and 3 million voters were turned away from the polls without casting a ballot on Election Day 2000. I would like the second panel of today's witnesses to highlight the steps that are being taken to ensure that all aspects of HAVA are being followed, in order for the American people to have the best election possible this November.

My concern is that all of the attention that is being given to voting security will inadvertently suppress voters from coming to the polls if they feel their votes will not count. What steps are election officials taking to fix registration problems? Will they have enough provisional ballots for voters?

Two-thirds of the public will vote on the same type of equipment they used in 2000. I'd like the second panel to review what is being done to ensure that all voting equipment is secure? What steps are being taken to inform the public that DRE machines are counting ballots correctly?

I am also interested in hearing the witnesses' assessment of recent New York Times' editorials calling into question the views and actions of the senior Senator from Connecticut and one of chief authors of HAVA, Chris Dodd; and Jim Dickson, Vice-President for Governmental Affairs for the American Association of People with Disabilities, who are trying diligently to improve the election process.

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

###

The CHAIRMAN. I guess the ranking member Congress is insinuating that Congress is a little bit like jeopardy?

Mr. Ehlers.

Mr. EHLERS. Thank you, Mr. Chairman. And thank you for having this hearing on a very important topic. It has reached the popular press. There is an article in PC World this month entitled "Is E-voting Safe?" so obviously, people are beginning to worry about it and their conclusion is, as many of us have concluded, not totally safe. We clearly have to do a better job of ensuring the security, reliability, usability and verifiability of electronic computers in voting. And I don't want to go into all the details, but I am very concerned as someone who has programmed computers and who understands how one could hack these or change results or flip votes, as the case may be.

This clearly is an area of concern. The closed source code is one of the problems, because something may have been inserted in the source code, which would allow a flipping of votes. But there are many other problems and issues that have to be addressed as well. So I thank you for holding this important hearing. I look forward to hearing from the witnesses, some of whom I have heard from before. And I hope that we learn something from it. Let me add one other factor. One of the biggest disappointments in HAVA to me has been the lack of funding for the National Institute of Standards and technology to set the standards. And once again, we are going to have a bill on the floor today, which does not provide funding for the National Institute of Standards and Technology to set the standards and make—and to me that is one of the most important things we should be doing because we have to be concerned that these machines work properly, that they are not tinkered with, that there is no fraud, either intentional or accidental that is taking place.

And so I hope with the assistance of Mr. Hoyer, who is on the Appropriations Committee and some of my other friends, that we can change this as the appropriations bill goes through the process and provide adequate funds for the National Institute of Standards and Technology to lend its expertise to this issue. I yield back the balance of my time.

The CHAIRMAN. I would note the gentleman, Mr. Hoyer—and we set this last hearing on the overall issue—has been diligent. And when we put this bill together—I am speaking we, everybody—we didn't want an unfunded mandate. And we have had parts of the funding due to Mr. Hoyer's diligence and the Speaker and other people who have been active on this, such as Senator Dodd and Senator McConnell. But there is more to do. And as we said at the last hearing, it has to happen. It just absolutely has to happen. Mr. Brady.

Mr. BRADY. Thank you, Mr. Chairman. I do want to recognize and thank our leader, Steny Hoyer for being here and keeping up his participation and his interest. And it is also enlightening to accommodate a fellow member, Mr. Rush Holt that asked to speak, but I also have to respect our chairman and ranking member who would have this place filled up with 430-some of us that all want to talk on this issue. I have to recognize the knowledge that you have in this field and also the bill you have in front of us and you

experienced it firsthand in your election. And I do appreciate your participation and your interest. Thank you, Mr. Chairman.

The CHAIRMAN. Mr. Mica.

Mr. MICA. Thank you, Mr. Chairman, and I thank you for holding this hearing. Our Committee on House Administration has an important responsibility to see that our election system works. Quite frankly, I am a bit frustrated by our continuing to throw money at some of these problems. I have always viewed the elections responsibility as that of State and local with Federal participation where we can assist. One of the things we don't have any problem with in Congress is throwing huge amounts of money at problems. And I think we started off with \$3.9 billion for this program. And we have adopted some systems, for example, electronic voting and also optical readers replacing punch cards that were used in Florida and other places and lever voting equipment. With new technology like cell phones—

The CHAIRMAN. Was that the President?

Mr. MICA. Actually, I have very strict instructions. It could have been the President. But it wasn't, it could be the Secretary of Transportation. I am heavily involved with issues there. But the most important person is my septic tank operator.

The CHAIRMAN. We will move on with the topic.

Mr. MICA. In our business you have to put things in priority. But, again, we spent a lot of money. I did not support this, the act or the huge amount of money that we threw at the problem. In Florida, I participated in some of the recount. And I saw that in one of my counties, we had optical readers which we are spending a portion of this billions of dollars to replace punch cards and also lever, old lever equipment, which actually don't work that badly when you look at some of the problems we have seen with the newest equipment. But I remember looking through hundreds of ballots. And the optical reader is a very simple thing. It has an arrow like this and you just fill in this little space here.

Now that seems like a pretty darn simple thing to do. And I am telling you, hundreds of people—they circled entire areas. They x'd down through. They destroyed a ballot. Unfortunately, I think what you need is a more intelligent electorate. So we are replacing this equipment—we are replacing this equipment now and there is less than 1 percent error rate improvement in putting these machines in, and we have got the electronic equipment that this hearing is about. We found now we are buying this very expensive electronic equipment. And I think it was in Virginia, the dummies didn't plug the machines in. So now we have to pay for training courses to plug these in.

My cell phone just went off and having been in the communications and cellular business, I know all the problems you can have with electronic equipment. And I can tell you we will be back here to fund auxiliary power units to ensure that the backup to run the paper trail or the electronic equipment that was to replace the equipment that we just spent other money on. So I would like to see the system work. Some of the best equipment is actually the lever equipment, the most primitive, but some of the most accurate that was ever produced and we are replacing it, again, at great expense.

So I am discouraged that we have spent a lot of money on a system that doesn't work. I think we have got to do a much better job of educating people. And no matter what system you put in place, you are going to have problems in the future. And there will be people who will use that equipment, whatever we put in and misuse it and their vote will not be counted. It has been that way. It is that way. And it will be that way. So I thank you for holding this hearing and I hope without spending too much hard earned taxpayer money, we can find some solutions that work. Thank you.

The CHAIRMAN. Thank the gentleman. On the first panel, we have Dr. Avi Rubin, Professor of computer science at Johns Hopkins University; Dr. Brit Williams, professor of computer science and information technology at Kennesaw State University; Tadayoshi Kohno, computer security expert with the computer science and engineering department at the University of California at San Diego; and Dr. Michael Shamos, Professor in the School of Computer Science at Carnegie Mellon University. I want to welcome all of you to the Hill.

STATEMENTS OF AVI RUBIN, PROFESSOR OF COMPUTER SCIENCE, JOHNS HOPKINS UNIVERSITY; DR. BRIT WILLIAMS, PROFESSOR OF COMPUTER SCIENCE AND INFORMATION TECHNOLOGY, KENNESAW STATE UNIVERSITY; TADAYOSHI KOHNO, COMPUTER SECURITY EXPERT, COMPUTER SCIENCE AND ENGINEERING DEPARTMENT, UNIVERSITY OF CALIFORNIA AT SAN DIEGO; AND DR. MICHAEL SHAMOS, PROFESSOR, THE SCHOOL OF COMPUTER SCIENCE AT CARNEGIE MELLON UNIVERSITY

The CHAIRMAN. And Dr. Rubin, we will start with you.

STATEMENT OF AVI RUBIN

Mr. RUBIN. Good morning, Chairman Ney, Ranking Member Larson, and members of the committee. My name is Avi Rubin and I am a computer science professor at Johns Hopkins University. I am going to start with two things that may surprise you in order to highlight the points that I think are important. I am not fundamentally against electronic voting. The second is that a DRE retrofitted with a paper trail is not necessarily the best kind of voting machine that we can have. There are ways to design and build systems so that those who make and those who administer the machines will have a tough time cheating.

Today, DREs are not being produced this way. The advantages of a well-designed system is that they do not require complex procedures in order to ensure security. They take control of the outcome out of the hands of the manufacturers and the vendors and they take into account the needs of users including special needs users. The elements of such a system are transparency in the form of open code, so people can see what is going on inside of a machine. Independent audit, that is an audit that is not controlled by the designers of the system peer review, which is fundamental to computer security and usability system to make sure everybody who needs to use the machine can use it and it is designed appropriately. There are many attractive features of DREs that are often touted: Accessibility for those who do not speak English as the pri-

mary language or for blind people; user friendliness of the machines; the ability to catch undervotes and warn the voter and the ability to prevent overvotes and the results are available immediately.

If I were given these requirements and asked to design a voting machine with these properties, it would not be like today's DREs. My focus is always security, but you can achieve all of the properties that I just mentioned much more securely.

Here is how I would design a voting machine. The machine would be as accessible as a DRE. It would be as user friendly. It would warn about undervotes. It would prevent overvotes. But there would be some big differences. Meaningful recounts would be possible, it would be incredibly difficult for a vendor to rig the election, and voters would be able to have confidence in how their vote was recorded.

Now the interface, as far as a voter is concerned, would be the same as a DRE, but I would name the machine a ballot preparation machine. You walk up to the machine, and you have exactly the same experience you would with a DRE. You touch all your selections, but at the very end of the experience, instead of "cast vote," you would push "print ballot," and the machine would output a card maybe similar to a boarding pass you would get at the airport these days or, if there were a lot of choices, maybe it would be an 8-by-10 card and that would be the ballot.

The voter would review the ballot to see if their markings and their choices corresponded to what they intended; and, if it did not, there would be a shredder available to shred that and they could do it again. Perhaps they made a mistake or perhaps something was wrong with the machine. In either case, it would be good to know that.

Now we have a separate problem on our hand, a completely separate issue, which is how do we count the ballots. Some places say, well, we have these paper ballots. We have had a simple election. Let us count them by hand. Other places may say our ballots are too complicated. What we can do is feed them into a completely different unit which would be an optical scanning unit that could read it in and count the votes.

You may say, well, that is a computer, too. I would respond I am not opposed to electronic voting. The difference is if you optically scan these things, you are dealing with a much simpler machine. It could be several hundreds lines of codes, could be open source and at the end of the day you have the ballots.

Let me stress the big difference between a DRE with a—versus the kind of machine that I am describing. In the kind of machine I am describing, there is only one authoritative ballot, and that is that piece of paper. In a DRE that you retrofit with a verifiable paper trail, which is better than a DRE without it, but you have the issue of having two different votes. Do you count the electronic ones? Do you count the paper ones? I think there should only be an authoritative paper ballot, but we can utilize computers to create that ballot, and we can utilize computers in order to count those ballots and utilize the paper to check that count.

I am quickly running out of time, so let me draw an analogy, and I started about 10 seconds late. The grading system we use to turn

in our grades at Johns Hopkins is done over the Internet, but it was done with security in mind. And I am perfectly happy at the end of the semester uploading my grades to a central server at Johns Hopkins, even though, considering you have a bunch of computer science students who might try to hack the system, it is a lot less work to do that than to work for a grade in all your classes.

Why am I willing to do this? Because the following semester, direct from the Registrar's Office, hand walked to me by the secretary, is a paper with grades on it that were recorded; and I get to compare them to the grades that I submitted and say, did anybody alter these grades, have they been tampered with? And I know that, if they have, I will catch that.

In DREs, we don't have a catch like that. The only point at which we can perform an audit which the voter can verify that the vote was recorded correctly is when they are voting and they have to have an ability to look at the actual ballot and say that is how I voted. Thank you.

The CHAIRMAN. Thank you, Doctor.

[The statement of Mr. Rubin follows.]

Testimony, U.S. House committee on House Administration
1309 Longworth House Office Building

Dr. Aviel D. Rubin, Professor of Computer Science
July 7, 2004

My name is Avi Rubin. I am a Professor of Computer Science and Technical Director of the Information Security Institute at Johns Hopkins University. I am author or co-author of several widely used books on the subject of computer and network security, and I have chaired several of the top security research conferences. I received my Ph.D. in Computer Science from the University of Michigan in 1994 in the specialization of Computer Security. I have been researching security issues related to electronic voting since 1997. Last year, by invitation of the Department of Defense, I served on the security peer review group of the SERVE voting system for absentee voting for military personnel and overseas civilians. I also participated as a panelist in the 2000 National Science Foundation study of the feasibility of electronic voting. Last year, my research team analyzed the code used in the Diebold Accuvote TS and TSx and wrote a report citing many security flaws that we found. Our study was published in the top peer reviewed computer security conference, the IEEE Symposium on Security and Privacy. I am a member of the National Committee on Voting Integrity, and in March, I served as an election judge in Baltimore County where Diebold Accuvote TSx machines were used.

I am here as an expert in a particular domain, namely computer security. I recognize that voting is a complicated issue with a diverse set of values, each of which is very important to the functioning of this process in a way that is reliable and trustworthy in the broadest sense. Security is a necessary component of a fair and accurate election process. However, there are other equally important components. Making sure that everyone can participate in a way that is private and independent is also key to our electoral process. Making sure that people from all walks of life can participate in the process in a language they can comprehend is also important. An accurate and secure system that limits the ability of individuals with disabilities and language minorities would fall short of meeting the goals of our democracy, as would a system that allowed everyone to participate but failed to protect the integrity and accuracy of their vote. Luckily, security and accessibility are not competing goals. While today's DREs increase accessibility, they do not provide adequate security. Appropriately designed voting systems, can provide accessibility and security. Our commitment to a fair, inclusive, secure election process requires us to demand both from our election machinery.

I come before you today to contribute my expertise garnered over years of experience. Given that we all agree that security is an important component of elections, I ask that you hear me and understand the serious nature of my critique of current DREs.

My primary concerns with today's DREs are:

- There is no way for voters to verify that their votes were recorded correctly.
- There is no way to publicly count the votes.
- In the case of a controversial election, meaningful recounts are impossible.
- The machines must be completely trusted. They must be trusted not to fail, not to have been programmed maliciously, and not to have been tampered with at any point prior to or during the election. We have techniques for building secure systems, and they are not being utilized.
- With respect to the Diebold Accuvote TS and TSx, we found gross design and programming errors, as outlined in our attached report. The current certification process resulted in these machines being approved for use and being used in elections.
- We do not know if the machines from other vendors are as bad as the Diebold ones because they have not made their systems available for analysis.

Since our study came out, three other major studies often referred to as the SAIC report, the Ohio reports, and the RABA report, all cited serious security vulnerabilities in DREs. RABA, which is closely allied with the National Security Agency, called for a "pervasive rewrite" of Diebold's code. Yet, the vendors, and

many election officials, such as those in Maryland and Georgia continue to insist that the machines are perfectly secure. I cannot fathom the basis for their claims. I do not know of a single computer security expert who would testify that these machines are secure. I personally know dozens of computer security experts who would testify that they are not.

I have been disappointed that the policy community did not reach out to the computer security community when making decisions about voting technology, and when my community came to the table, they said it was too late. At this point the failures of current DREs have been documented in four major studies by leading computer security experts, and we have ample field experience documenting failures at the polling place. Yet computer security experts, myself included, find ourselves routinely referred to as luddites and conspiracy theorists. Failing to confer with computer security experts in decisions about voting technology was a mistake. Given the gravity of the security failings the computer security community has documented in current DRE systems it is irresponsible to move forward without addressing them.

Addressing the problems I and others have documented with DREs requires more than just fixing the machines. We must reform the process for establishing voting technology to provide transparency. Vendors are not subject to public code review. In the one instance where independent security experts had an opportunity to examine a voting system, the results proved that the current process results in machines being deployed with unacceptable lack of quality control. We cannot achieve perfectly secure systems; such things do not exist. But on the spectrum of terrible to very good, we are sitting at terrible. Not only have the vendors not implemented security safeguards that are possible, they have not even correctly implemented the ones that are easy.

The defenders of the DREs do not account for the ease with which a malicious programmer could rig an election. It is much easier to hide malicious code in software than it is to detect it. Without an external check on the system, a fully electronic voting machine cannot be properly audited. Research needs to be done on how to design auditable and voter verifiable elections. The best way to achieve this today is with a paper ballot that voters can verify. There is no reason why touchscreen machines cannot be used to generate ballots, but they should not be used to tally votes. The tallying software should be as compact as possible, and it should be available to the public for inspection.

I'd like to stress one important point. Security and functionality are completely different things. Functionality is whether or not something works when it is used as planned. Functionality can be tested, and the tests can be used to make predictions about the future behavior of a system. Security, on the other hand, has to do with how a system behaves under unanticipated circumstances with an active, dynamic adversary trying to subvert it. By definition, you cannot test a system for security the way you test for functionality. It is inappropriate and incorrect to draw conclusions about the security of a system based on its past performance. The fact that this argument is consistently put forward in defense of the security of the DREs demonstrates just how much real security expertise is needed in this process. You would not design a heart implant without feedback from cardiologists. You would not design defense systems for the physical security of this country without consulting military experts, and you should not design systems for computerized elections in this country without consulting computer security experts. I can assure you from my analysis of the Diebold machines that no such expertise was utilized.

In conclusion, my colleagues and I have presented our analysis to many different groups of computer scientists, including the National Science Foundation, the National Academy of Science, and several security conferences. We have won awards for this work, and the community at large is in strong agreement with our conclusions. I recommend that you continue to seek broad input from the computer science and the computer security communities. These people have a long history of experience with designing mission critical systems. The opinions of the experts in this matter are quite different from the picture being painted by the vendors and some state officials, all of whom have much less expertise, or no expertise whatsoever, in computer security.

The CHAIRMAN. Dr. Williams.

STATEMENT OF BRIT WILLIAMS

Mr. WILLIAMS. As you mentioned in your remarks, after the 2000 election, a group of political activists began to attack the direct recording systems, claiming that they are totally unsecure, that they can't be made secure and the only way you can make them secure is with the addition of a verified paper ballot. When this was picked up by some of my fellow computer scientists, it gained attraction in the media.

The claim is that we cannot build a secure voting system. Now a DRE voting system—or any voting system, for that matter—but a DRE voting system is one of the simplest computer applications you can imagine. The main line is to recognize a touch on a particular location on a screen and add one to the appropriate register. That is it. It doesn't do any complex computations, doesn't take the logarithm or the trigometric functions of anything. It doesn't do square roots, doesn't multiply or divide. And to claim that we can't build a secure accurate system just flies in the face of the way we live our lives. We fly on airplanes that are controlled by computers. Our sailors go under the ice cap on submarines controlled by computers. We have been to the moon and back on spacecraft controlled by computers. On a less grandiose scale, our cars, our microwaves, our watches are controlled by computers.

I am not saying we should not attempt to improve our computer systems. We should. And I like Dr. Rubin's system and I look forward to it, but we have to deal in the short term with what we have on the shelf right now. And there are many dimensions to a voting system other than just security. We have to look at availability, reliability, maintainability, usability and even affordability. Any change to the voting system, particularly something as drastic as adding paper receipts or paper ballots, needs to be evaluated in terms of the total voting system, not just the security aspects of it.

Now this—your HAVA legislation created the Election Assistance Commission system and gave them the resources and the authority to approach this in a very orderly and systematic manner, and I sincerely hope they will be allowed to do that.

Now we don't believe that we are in imminent danger. We think in Georgia that our voting system is both accurate and secure. We have measures in place to ensure that the voting system components, the computer components are as accurate and secure as current computer technology permits. We have physical security measures and the essential ingredients in DRE systems in place to compensate for the remaining vulnerabilities in the system. These are discussed in our written report, and I won't go into them here.

We have a Center For Election Systems at Kennesaw State University that provides technical assistance and training to our 159 counties. Before any piece of equipment can be used in an election in Georgia, it has to be examined by members from this center. And, in addition to this testing, we now, out of the center, offer training for election managers, for new election poll workers and for board members, election board members.

So let me close by pointing out that we do not live in an absolute world, that everything we do contains a certain amount of uncer-

tainty. When we fly on an airplane, we know there is a remote possibility that we won't live to reach our destination. When we drive our cars, we know there is a possibility we won't reach our destination. We evaluate the risk and the advantages, and we make a decision.

Now we do the same thing with our election in Georgia. We know when we conduct an election that there is a remote possibility that someone has altered that election in an attempt to defraud or disrupt the election. But we also know the diligence with which we maintain and protect the system and we know that we reduce that risk to a miniscule level.

In our written report, we point out that we think that we can detect an alteration of that system with a chance of less than one in one billion. So with that kind of a risk, we are willing to go ahead and hold our election with a voting system that allows a business person to vote on their lunch hour very quickly and easily, that provides the elderly and infirm with a voting interface that does not require difficult manipulation, that allows a non-English-speaking voter to vote in their native language, that allows disabled voters to vote unassisted, many of them for the first time, that reduces the rate of incorrectly marked ballots by a factor of five and provides a level of accuracy that exceeds any voting system that has previously been used in the State of Georgia.

Now no one that is involved in elections would come before you and claim that the current systems are the best that can be devised or suggest that we can't make improvements. We have a culture of continuous improvement, and we applaud people who offer reasonable, well-reasoned criticism and who have carefully considered recommendations for improvement.

I thank you for this opportunity to speak to you, and may God bless America.

The CHAIRMAN. Thank you.

[The statement of Mr. Williams follows:]

**Testimony before the
House Administration Committee
By
Kathy Rogers, Director, Georgia Elections Division
and
Britain J. Williams, Ph.D., Professor Emeritus
Of Computer Science and Information Technology
Kennesaw State University**

July 7, 2004

Introduction

The 2002 General Election was a milestone in Georgia history, as we became the first state in the nation to successfully implement a statewide uniform system of electronic voting. Georgia's transition to new electronic voting equipment was the result of an in-depth analysis of the accuracy and accessibility of available voting systems, an extensive statewide voter education program and poll worker training, and an unprecedented partnership between state and county governments.

In the almost two years following that first election, Georgia counties have conducted hundreds of elections using electronic voting. Numerous success stories have emerged from nearly every corner of the state. Two themes quickly emerged: Georgia voters young and old embraced and expressed confidence in the new voting system, and our state's under-vote rate was dramatically reduced following the deployment of the electronic voting platform. Georgia voters have overwhelmingly indicated their approval of electronic voting in not one but two independent public opinion studies conducted by the University of Georgia's Carl Vinson Institute.

In recent years a small group of political activists captured the attention of the media with the conjecture that direct recording electronic (DRE) voting machines are inherently not secure. Furthermore, they contend that the only way that these systems can be made secure is by the addition of a Voter Verifiable Paper Ballot (VVPB). These activists' conjectures gained respectability when they were joined by several computer scientists from major universities. These academics claim that computer systems in general and voting systems in particular cannot be made secure.

A DRE voting system is a comparatively simple computer application. The main line of the system is to respond to a touch at a specific location on a touch-sensitive screen and add one to the appropriate register. There is no requirement for intricate or complex computations. There is no requirement to compute any logarithmic functions, trigonometric functions, or even take the square root of anything.

The conjecture that using current technology we are unable to make such a simple system secure and accurate is contradicted by the facts of our daily existence. We build secure

and accurate computer systems that fly our airliners. We build secure and accurate computer systems that guide our submarines under the ice cap. We build secure and accurate computer systems that guide our astronauts to the moon and bring them safely back to earth. We submit to open heart surgery while a computer monitors our vital signs and controls an artificial heart and lung machine. The list of secure and accurate computer systems that monitor, control, and improve our lives is large and growing daily.

This is not to imply that our current DRE voting systems do not need to be improved. They do. But there are many aspects to a voting system other than accuracy and security. These include availability, reliability, maintainability, usability, and even affordability. Any change to a voting system must be evaluated on the basis of its impact upon the entire system. To this end Congress has created the Election Assistance Commission (EAC). This Commission has the resources and authority required to affect an orderly and disciplined evaluation of the state of the existing voting system technology and implement improvements to voting systems in an orderly manner.

The evidence is compelling that a rapid, poorly formulated forced addition of a paper ballot or receipt to the existing DRE voting systems is unnecessary and could have adverse consequences that far offset any perceived advantages. There is, in fact, no credible evidence that we are in imminent danger of a corrupted elections process created by new DRE voting systems. There is sufficient time, and a clear rationale, to allow the organizations and processes defined in the Help America Vote Act to perform their assigned duties and responsibilities.

To understand our perspective in Georgia and why we so strongly advocate the advantages of current generation electronic voting technology, it is important to know where we've been and why we took the path towards a uniform statewide DRE system.

Georgia's 2000 Election Experience

The 2000 Presidential Election served as a huge wake up call to a nation of voters and election officials. Alarmed by the high percentage of under-votes recorded by voting equipment in Florida, Georgia Secretary of State Cathy Cox compiled data on under-votes that occurred with Georgia's then existing voting equipment; a mix of lever, punch-card, optical scan and even paper ballots. The findings of that study were staggering. Not only did Georgia have a higher under-vote rate than Florida; at 3.5% our under-vote rate far exceeded the national average of 1.9% and was reported by the CalTech/MIT study as the third-highest in America. A study entitled "A Wake-Up Call for Election Reform and Change" was subsequently produced by the Secretary of State outlining the performance of Georgia's election equipment in each of its 159 counties during the 2000 General Election. Further analysis documented extremely large variations in under-vote rates between counties, as well as large under-vote variations between majority vs. minority precincts in the same county using the same equipment. In 2001 the ACLU, on behalf of several Georgia voters, sued the state, noting that, based upon the state's own data; the election platform then in place had a discriminatory impact and served to disenfranchise minority voters in counties throughout the state.

The findings in the “Wake Up Call” report were alarming enough that in 2001 the Georgia General Assembly passed, at the request of the Secretary of State, Senate Bill 213 which provided for the creation of a 21st Century Voting Commission. This group was tasked with studying the accuracy and reliability of all nationally qualified voting systems and to provide a report on its findings and recommendations to the General Assembly. This Commission was comprised of a balanced, multi-partisan group of General Assembly members, election officials, technology experts, and other important stakeholders. The commission invested a significant amount of time studying reports on existing technology, visiting other states to observe elections using electronic voting systems, holding meetings to obtain public comment, and, most importantly, overseeing an electronic voting pilot project.

In November 2001, 13 cities participated in a pilot project, utilizing six different NASED-qualified and state-certified DRE systems from six different vendors, to conduct actual municipal elections. The cities were selected to assure geographic, demographic and partisan diversity. The University of Georgia’s Survey Research Center was retained to perform an intercept, or “exit poll,” of voters to measure their reactions to the equipment and attitudes about the deployment of new voting technologies.

Altogether, the State conducted a full year of study, evaluation and due diligence before making its recommendation for voting system reform. In January 2002 the 21st Century Voting Commission unanimously recommended to the Governor and General Assembly that Georgia adopt a statewide uniform system employing electronic voting equipment.

Election Day 2002

November 2, 2002 was an historic day for Georgia. For the first time, every voter was afforded the opportunity to cast a ballot in the same manner using the same equipment with precisely the same voting interface. A voter in one county did not receive the advantage of better technology while his counterpart in a neighboring county voted on antiquated voting equipment prone to high error rates. That fact sometimes seems to be forgotten today. By upgrading its voting platform Georgia corrected a problem that was close to being a disaster.

In that single day many concerns and fears were laid to rest; the elderly did not have difficulty voting and voters were not afraid of the new technology. Blind and visually-impaired voters who had previously never cast a ballot independently expressed their feeling of pride and accomplishment at being able to utilize the features of electronic voting that allowed them to vote unassisted for the first time.

Electronic voting has removed the opportunity for fraud and error that inevitably comes when humans record votes on paper and handle and count paper ballots. In light of the current clamor for the addition of a paper receipt, it is worth noting that every single documented case of election fraud in recent Georgia history has involved the use of a paper ballot.

Georgia has taken huge strides in improving accuracy and ease of use, and the data gives us reason to be confident that a much higher percentage of the ballots cast in Georgia in November 2002 represented a true and accurate reflection of the voter's intent. Voters are allowed to review their ballot prior to touching the cast ballot button. No system has ever provided that capability before.

Six years ago, under Georgia's antiquated voting platform, the top-of-the ballot U.S. Senate under-vote was 4.8% of ballots cast. In 2002, after deployment of the new electronic system, the under-vote in the top-of-the ballot U.S. Senate race (an "apples to apples" comparison of system performance) was a mere 0.87 percent. That is a more than five-fold reduction in under-voting, a decrease of 71,000 ballots that showed no choice in the top of the ticket race. This is clear and convincing evidence that an electronic voting platform that prohibits over-votes, that provides the voter with feedback and that offers a summary screen to check and review ballot choices can dramatically improve the accuracy of the vote count.

Voter Confidence Validated

The Carl Vinson Institute of Government at the University of Georgia conducted a public opinion survey following the 2002 General Election and found that Georgians overwhelmingly prefer electronic voting to other methods. More than 70% of respondents reported being "very confident" that their vote was accurately counted, a sharp increase from the 56% who responded to that same question during the 2001 pilot project. Some 97% of voters said they "experienced no difficulties" when using electronic voting terminals.

The Vinson Institute followed up with a second survey one year later, in November 2003, which confirmed that over 70% of voters are still confident in Georgia's electronic voting platform. This same survey also noted that all voters in all age groups, income and education levels, and racial and ethnic groupings believe that electronic voting is superior to forms of voting previously used in Georgia.

The Arguments For, and Against, Voter Verifiable Paper Ballots

Those who distrust current DRE voting systems and believe they are easily manipulated to create fraudulent election outcomes have prescribed what they claim is foolproof solution: the addition of a paper receipt, or voter verifiable paper ballot. These claims warrant close examination.

When we vote to elect the members of the board of directors of a company, to elect the officers of a social or civic club, or to elect the officers of a labor union we cast a "ballot" (sometimes called a proxy). This ballot contains unique identifiers such as a signature, social security number, or member number that can be used by the election monitors to

validate the ballots. Given the ease with which the individual ballots can be validated it is unusual for the persons conducting these types of elections to expend the effort and expense necessary to purchase and implement a commercial, NASED Qualified voting system. They typically gather the votes and use their in-house computer technicians to develop a system to tally the votes. Any anomaly or challenge can be resolved by resorting to the verified ballots.

When we vote in a municipal, state, or federal election we do not cast a ballot in the manner described above. We cast a “secret” ballot, and this is an essential distinction. This ballot, by law, can contain no unique identifier that will enable anyone, including the voter, to identify the person who cast the ballot. Thus, in a municipal, state, or federal election there cannot exist a truly “Voter Verifiable Ballot”, paper or otherwise

The only paper output that can be added to a DRE voting system is the capability to produce a paper “receipt”. There are at least three DRE voting systems in the process of obtaining NASED Qualification that have the ability to produce a paper receipt. These systems demonstrate the problems that can result from attempts to implement modifications to a voting system in the absence of clearly defined, well thought out standards.

The EAC Voting System Standards (formerly known as the FEC Voting System Standards) do not currently contain a specification for a paper receipt produced by a DRE voting machine. The voting systems that produce paper receipts are being NASED Qualified under a provision of the Standards that permits optional features. In particular, the Standards require that a voting system comply with its own documentation. If the voting system documentation defines an optional feature (i.e. a printed receipt) then the Independent Test Agency (ITA) verifies that this feature is implemented in the system exactly as defined in the documentation.

As a result, the paper receipts produced by the voting systems currently seeking NASED qualification do not comply with the EAC Standards requirements for a ballot. For example, these systems will not comply with the Standards requirement for high contrast or increased print size to accommodate a person with impaired vision. Also, they will not comply with the Standards requirement to produce ballots in multiple languages.

Operational Considerations of Adding Paper Receipt

Experience has taught us that the deployment of a significant new addition to a DRE platform must also be examined in the light of Election Day reality. The success or failure of any voting system rests on the shoulders of poll managers and poll workers, who are, after all, citizen volunteers, many of them elderly, paid a very modest sum to operate voting equipment perhaps only once or twice a year. Paper receipt advocates who compare them to employees at WalMart or Target miss the mark entirely - poll workers are not and never will be full-fledged employees, who can expect regular sessions of training and who have multiple levels of professional supervision at their workplace. Therefore, not only must poll workers be carefully trained, but equipment

must be designed to minimize the technical and operational requirements they need to master in order to carry out a successful election. If, because of the demands of new and more complicated equipment that includes printers and related components, even one percent of Georgia precincts experience problems making their polling places operational on election morning, that translates into more than 30 precincts unable to allow voting to take place; a situation that no doubt would be portrayed by the media and perceived by the public as a catastrophic failure.

Just as important, we should make absolutely certain that the addition of a paper receipt function, if implemented, does not put us back into unacceptably high under-vote rates that we have worked so hard to overcome. In the sterile environment of a computer science laboratory, a new paper receipt prototype may appear simple and fool proof. But in the real world of elections, with equipment that must be accessible to voters with widely divergent levels of education, literacy, language proficiency, experience and physical ability or disability, it is crucial that the user interface be simple, straightforward and intuitive. Georgia spent enormous time studying this very issue, and the experience of other jurisdictions, before adopting a modern DRE platform as its preferred model. That due diligence paid off with plummeting under-vote rates - across all demographic groupings - and a much more accurate election outcome that re-enfranchised tens of thousands of voters. It would be tragic if a hurried, and inadequately researched, requirement for a paper receipt function makes the voter interface so complicated that it increases voter confusion and drives back upward the incidence of under-voting.

We Are Not in Imminent Danger

Computers have been used to tally elections in America since October, 1964 when DeKalb County and Fulton County, Georgia were the first jurisdictions in America to employ a punch-card voting system. Since then the State has used every type of computer-based voting system: punch-card, central count optical scan, precinct based optical scan, and direct recording electronic voting systems. During these forty years there have been many attempts to defraud a Georgia election, but not a single one of these attempts has involved an attack on the computer system. This is probably due, at least in part, to the fact that many people believe that they know how to successfully alter a piece of paper, but very few people believe that they have the ability required to successfully alter a computer system.

The Georgia DRE voting system is both accurate and secure. Measures are in place to insure that the voting system computers are as accurate and secure as current computer technology permits. In addition, physical security measures, an essential ingredient to secure elections and a topic that is often ignored by the critics of DRE systems, are in place to compensate for the remaining vulnerabilities that have been identified in the computer system. An extensive, statewide training program has been implemented to prepare our election officials and poll workers to recognize and react to any problems that may occur during the course of an election.

The Role of the KSU Center for Election Systems in Georgia

The Center for Election Systems at Kennesaw State University was created in 2002 to provide support and independent testing to all 159 Georgia counties. The Center for Election Systems at KSU tested every touch screen unit, encoder, optical scan ballot reader and server used in the 2002 General election. Tens of thousands of voting terminals and related components were tested by the Center, and its staff continues to travel to each of Georgia's 159 counties to independently test and validate all new equipment purchases.

In addition to testing, The Center for Election Systems now offers support to counties and their staff in the areas of poll worker training, enhanced courses on election management training, and courses for new election officials.

Election System Security Has Multiple Components

Those who are charged with conducting elections understand that the security of an election does not rest on the performance of equipment alone - whatever that voting platform may be. These election experts are well acquainted with the entire umbrella of security that surrounds the voting process. Every feature of the comprehensive security protocol, including paperwork procedures and physical security, is important to assuring the integrity of the voting process. A secure and accurate election begins long before Election Day and is comprised of many levels and layers of testing.

Computer System Security in the Georgia Voting System

Georgia has been a full participant in the EAC Voting Systems Standards project since its inception. Before a voting system can be considered for use in Georgia, it must be examined by the ITAs for compliance with the EAC Voting System Standards. Georgia considers a voting system to consist of a specific version of each of the system components: hardware, voting system software, and operating system software. Any change to any component, no matter how insignificant, is considered a different system and requires re-examination, both NASED Qualification and State Certification, of the entire system.

When a voting system successfully completes ITA qualification testing and is issued a NASED qualification number, it can be brought into Georgia for State Certification Testing. The system to be tested is not obtained from the vendor but is transmitted to the KSU Center for Election Systems directly from the ITAs.

The KSU Center for Election Systems conducts a series of tests on the system. Some tests examine the level of difficulty associated with operating the system. Another tests the capacity of the system to accommodate the maximum number of ballots that might be cast in a large precinct or at an in-person absentee voting location. One test is specifically designed by the KSU Center for Information Security, Education, and Awareness to detect fraudulent or malicious code that might be present in the system. This test is designed to wake up any, so called, Trojan horse that might be present. In all

of these tests a known pattern of votes is cast and compared with the output of the system.

If any of these tests result in a modification to the system, the entire system is returned to the vendor for correction and the NASED Qualification/ State Certification test cycle is repeated.

When the system successfully passes State Certification and is certified for use in Georgia, the KSU Center for Election Systems prepares an electronic signature of the system and archives the software source code and object code. The vendor is then authorized to install the system in the 159 county election offices. The primary reason for allowing the vendor to perform the installation is to protect the warranty on the system.

When the vendor notifies the State that they have completed installation in a particular county, the KSU Center for Election Systems sends a team to the county to conduct Acceptance Tests. These tests verify that the hardware is operating correctly and that the correct version of the software has been installed. During these tests the electronic signature of the software installed in the county is compared with the electronic signature of the software archived by the KSU Center for Election Systems to validate that the county system is identical to the system that was State certified.

The following describes three distinct objectives that are attained in order to insure the security and integrity of the Georgia voting system.

Objective 1: Verify that the voting system, as delivered from the ITAs, is free from extraneous or fraudulent code.

To attain this objective the KSU Center for Election Systems performs the following activities:

- Setup and conduct sample elections with known outcomes that are representative of Georgia general and primary election.
- Conduct high-volume tests to determine capacity limits of the system.
- Conduct tests to determine the systems ability to recover from various types of errors.
- Conduct tests to detect extraneous or fraudulent code.

Objective 2: Verify that the system as installed by the vendor in the local jurisdictions is identical to the system received from the ITAs and certified by the KSU Center for Election Systems.

To attain this objective the KSU Center for Election Systems performs the following activities:

- Prepare a validation program that will detect any changes to the system installed in the local jurisdictions.

- Run the validation program against the system installed in the local jurisdiction (after vendor installation).
- Provide the local jurisdiction with the ability to run the validation program.

Objective 3: Verify at specific and random times that the system has not been modified in any way.

Local Election Superintendents have the ability perform the following activities:

- Run the validation program immediately before beginning to define an election.
- Run the validation program immediately upon the completion of an election.
- Run the validation program after any suspicious event. Run the validation program at random times.

The validation program that is used to validate the correctness of installed systems is based on NIST certified SHA-1 contained in FIPS 180-2, August 2002 and includes the following:

32 bit CRC
128 bit MD 5 Hash
160 bit SHA-1 Hash

It is estimated that the chance of modifying the software in such a manner that this hash would not detect the modification is less than 1 in 1,000,000,000.

Procedural Security in the Georgia Voting System

Rigid policies and procedures are in place that control who can access to the election system, when they can access the system, what components they can access, and what function they are allowed to perform. The most familiar of these procedures is the process that a voter must go through in order to cast a vote on the system. Other procedures define the activities of election officials and poll workers.

Many of these procedures are directed toward insuring that the correct versions of the system software is initially installed in the election management system computers and voting stations and, subsequently, testing at various times to insure that this software has not been altered. We have already discussed this process.

Accuracy and uniformity of the ballots is critical to the success of an election. If a county so desires, the KSU Center will prepare the county ballot. Before the 2004 Presidential Primary Election the KSU Center prepared the ballots for 102 of the State's 159 counties. To achieve ballot accuracy and uniformity, the KSU Center for Election Systems reviews the ballot formats from all counties prior to each election.

Physical Security in the Georgia Voting System

The first line of security defense in any system is physical security. All other security measures go for naught if you leave the doors unlocked. The following is an overview of the physical security implemented in the Georgia voting system.

The election management system computers are kept in locked offices within the county election offices.

The election management system computers are not connected to any communication system, including the Internet, and contain no software other than the Windows operating system and its utilities and the election management system object code.

No person is allowed access to the election management system computer until his or her identity and purpose have been clearly established by the county Election Superintendent.

The voting stations are stored in their voting booth cases in locked county warehouse facilities.

At the precincts the PC memory cards in the touch screen voting stations are in a locked compartment on the voting stations. The Precinct Manager is the only person in a precinct with a key to this compartment.

After the polls close a printed report of the precinct results is posted on the precinct door. This places the results from the precinct in the public domain and any subsequent alteration of these results is easily detected.

The PC memory cards from a precinct are transported from the precinct to the county elections office by a sworn election official or a sworn law enforcement officer. Precinct managers may, at their option, send the precinct results to the county office via modem. However, these modem results are unofficial and are for the benefit of the press and the candidates. The official results are always computed directly from the memory cards.

The area of the precinct that contains the voting stations is secure. A voter is not allowed to enter this area until a voting station is available for his or her use. However, there are no enclosed voting booths and the secure area is in plain view of the poll workers, candidate representatives, party poll watchers, advocacy poll watchers, and media representatives. Any unusual behavior by a voter will be immediately detected.

Training and Ballot Building for Georgia Elections

One benefit of using a uniform technology throughout the State is that many ballot building procedures can be centralized. This enables better error detection and correction

as well as efficiency in the production of redundant ballot content (federal and statewide races and issues). Ballots can be reviewed for compliance with State law as well as proper district and precinct information. In the most recent statewide election the KSU Center for Election Systems prepared the ballots for 102 of the States' 159 counties. The KSU Center reviews all ballots, regardless of who prepared them, for accuracy and completeness. Following this review the ballots are returned to the counties for final review and acceptance.

The training issues in election technologies are unique. The process is heavily dependent upon personnel that are both volunteer and infrequent users of the system. The processes are a combination of manual and computerized operations that are the result of state and federal election law, state election rules, election tradition, and functional requirements of the election technologies. The processes are dynamic and change in varying degrees from election to election, requiring a constant vigilance of training objectives, materials, and curriculum. The KSU Center is responsible for working with the vendor and state and county officials in the development and maintenance of training programs.

In 2003 the State of Georgia enacted legislation that requires all election superintendents to successfully complete 64 hours of training. This training program includes election law, ethics, and election procedures, including those unique to the current DRE technology use in Georgia. This training helps to insure that appropriate security procedures are understood and implemented at the county and precinct level.

Conclusion

Members of this Committee as well as all election officials and policymakers have a difficult task - to sift through the rhetoric and headlines and accusations, some of them the product of partisan resentments - to separate fact from fiction and carefully assess the strengths and vulnerabilities of voting system alternatives. The claims and assertions of electronic voting opponents must be scrutinized with the same ferocity that has been applied to the statements and actions of equipment vendors and election officials. The successful experience of Georgia, and our enormous increase in accuracy and accessibility with minimal operational flaws and zero -not one - documented case of vote tampering or fraud - should be weighed as well.

No one knowledgeable about elections would come before you and claim that the current system are the best that can ever be devised, or suggest to you that we cannot make even more accurate, accessible and secure the systems that are now in use. A culture of continuous improvement is one that we have adopted in Georgia elections, and one that should be embraced by every jurisdiction. And so we applaud all those who offer responsible, well-reasoned criticisms and who have carefully considered recommendations for improvement. I am confident that this Committee will exercise great care and discernment in evaluating electronic voting systems, as we all strive to improve still further America's system of elections and voting.

Thank you for the opportunity to share my thoughts with this distinguished panel.

About the Authors:

Kathy Rogers is the Director of Elections Administration for the Georgia Office of Secretary of State. Ms. Rogers joined the Secretary of State's office in 2002 to spearhead implementation of the uniform touch-screen voting system adopted by the State of Georgia. Prior to joining the Secretary of State's team, Ms. Rogers served as the Election Supervisor for Chatham County Board of Elections (Savannah, Georgia). Ms. Rogers has almost two decades of election experience and has conducted elections with various types of voting equipment during her career. Ms. Rogers participates in several election organizations including the Georgia Election Officials Association, the National Election Organization known as IACREOT, the National Association of State Election Directors, the national Election Center, and also represents the State of Georgia on the newly created Help America Vote Advisory Board. Ms. Rogers recently graduated as a Certified Elections and Registration Administrator through a program administered by the Election Center and Auburn University.

Brit Williams is Professor Emeritus of Computer Science and Information Systems at Kennesaw State University. He was a consultant to the FEC during the development of the FEC Voting System Standards in 1990 and again in 2002. He is currently a member of the NASED Voting Systems Board and Chair of the NASED Voting Systems Board Technical Committee. He represents NASED on the newly created Help America Vote Technical Guidelines Development Committee. Dr. Williams has been conducting certification evaluations of computer-based voting systems for the State of Georgia since 1986. He also assists the states of Pennsylvania, Maryland and Virginia with certification evaluations of computer-based voting systems.

Brit Williams is Professor Emeritus of Computer Science and Information Systems at Kennesaw State University. He was a consultant to the FEC during the development of the FEC Voting System Standards in 1990 and again in 2002. He is currently a member of the NASED Voting Systems Board and Chair of the NASED Voting Systems Board Technical Committee. He represents NASED on the newly created Help America Vote Technical Guidelines Development Committee. Dr. Williams has been conducting certification evaluations of computer-based voting systems for the State of Georgia since 1986. He also assists the states of Pennsylvania, Maryland and Virginia with certification evaluations of computer-based voting systems.

The CHAIRMAN. Mr. Kohno.

STATEMENT OF TADAYOSHI KOHNO

Mr. KOHNO. Thank you, Chairman Ney and Ranking Member Larson and members of the committee, for holding this hearing today and for inviting me to speak on the topic of electronic voting security. My name is Tadayoshi Kohno, and I am a computer security expert with the University of California at San Diego's Department of Computer Science; and prior to joining the University of California for Doctor studies, I was a cryptography and computer security expert with two of the top cryptography and security consulting firms in the Nation.

Last summer, together with three other colleagues, I identified a number of security problems with Diebold's Accuvote TS electronic voting system. But I think that the most important result of our discoveries was that it concretely shows the existing certification processes are unable to identify security problems with electronic voting machines, and what this means is we have no reason to believe that other vendors' electronic voting machines are any more secure.

But what I would like to talk about with you today is why I, as a computer security expert, am deeply concerned about the use of existing paperless electronic voting systems. I want to emphasize that I am talking about existing paperless electronic voting machines because, you know, there might be the possibility of having secure enough paperless electronic voting machines in the future. I say "secure enough" because there is no such thing as absolute security. We don't have those machines today and won't have them by November, and let me expand on this. There are several reasons for this.

First, many people have suggested patching the existing systems, maybe by changing the software slightly or instituting new procedures. But this is not sufficient.

First, an analogy I always like to make is that spot treating security problems is like spot treating termites. You can never be sure that you have gotten rid of them all. And this is particularly important because when you hire a security analyst to look at the security of a system, you typically contract them for a limited period of time, and in that limited period of time they might only uncover the most obvious security problems. And while addressing the obvious security problems might raise the bar for an attacker, it doesn't mean you have addressed all the important problems.

Another thing that I want to point out is that unless all the components of the revised system, including the software and the revised procedures, are open to the public for public scrutiny and review, the public will have no reason to believe that the spot treatment actually succeeded in addressing the security problems; and I think this is illustrated most beautifully by the evolution of Diebold's Accuvote TS system. It is the system that we know the most about because it is the one that was analyzed publicly.

In response to our analysis, the State of Maryland hired SAIC and then RABA to conduct independent analyses of Diebold systems; and in both ours and SAIC's analyses we found that the Diebold system found a security problem in the way that the

Diebold voting terminals communicate with a back end server. Diebold tried to fix this problem. And then, in RABA's subsequent analysis, RABA found that Diebold's fix was insufficient.

I think the important lesson from this is that there are two points: One is that if Maryland had not commissioned RABA to conduct a subsequent analysis of Diebold's supposed fixes to our report, no one except for maybe an attacker would have uncovered Diebold's insufficient fix of the problems we identified. And I think, at a higher level, the thing I want to say, this begs the question. First, for systems the public cannot openly review and inspect, how or when can we know that a security problem has been accurately addressed?

I think in the remaining minute or so that I have that I would like to talk—I would like to advocate the following general principle; and that is, from a security perspective, the minimum requirement we should have for any new voting technology, it doesn't have to be computer technology, but the minimum requirement for any new voting technology is that it must be at least as secure as the technology that it is replacing. It is for this reason that our computer security experts are advocating the use of a voter-verifiable paper ballot, where we have the voting machines produce a paper ballot that the voter will look at and verify that it is correct and deposit it into the ballot box and that becomes the official record.

People have said that, you know, this has problems, too, because, you know, the ballot box could be stuffed, the ballots could be destroyed. But the point is that these are the problems that we already have with traditional paper-based voting mechanisms. By adding a voter-verifiable paper trail, we have not made things worse. Unfortunately, as a security expert, I cannot say the same thing about the use of existing paperless electronic voting machines in elections.

That is all the technical stuff I wanted to point out, but I wanted to thank the committee for focusing on this critical issue, and I think that the dialogue we are having today will move us forward towards addressing all of the security concerns.

The CHAIRMAN. I thank the gentleman for your testimony and the previous two witnesses.

[The statement of Mr. Kohno follows:]

**Testimony of Tadayoshi Kohno
Before the Committee on House Administration
U.S. House of Representatives
Hearing on Electronic Voting System Security
July 7, 2004**

Thank you Chairman Ney, Ranking Member Larson, and members of the Committee on House Administration for holding today's hearing, and for inviting me to speak on the topic of electronic voting security.

My name is Tadayoshi Kohno,¹ and I am a computer security expert with the Department of Computer Science and Engineering at the University of California at San Diego. I am also a Department of Defense NDSEG Fellow and an IBM PhD Fellow. Before joining the University of California for doctoral studies, I was a cryptography and computer security expert with two of the nation's top computer security firms, Counterpane Labs and Cigital. I have conducted security analyses for and provided guidance to a wide variety of organizations, ranging from billion-dollar corporations like American Express and VISA, to innovative new technology startups.

Last summer I was one of four computer security experts to analyze the design of Diebold's AccuVote-TS paperless electronic voting system.² As a consultant, I was accustomed to analyzing computer systems with poorly designed security mechanisms. But, since Diebold's machines had already been used in actual elections, I was initially expecting to find the AccuVote-TS system employing at least somewhat effective security mechanisms. I was mistaken. In our analysis we found that the implementers of the AccuVote-TS system ignored basic security best practices, and we found that the AccuVote-TS system was vulnerable to a number of simple and easy-to-mount integrity- and privacy-compromising attacks (details in our paper).

Although uncovering security problems with Diebold's machines was certainly important, I believe that the most important contribution of our work was highlighting the following two issues of great concern: (1) Because Diebold's machines had been certified, our discoveries show that *the current "logic and accuracy" testing and certification processes for electronic voting machines cannot be trusted to uncover even the most elementary security problems*. This means that there is no reason to assume that other vendors' certified electronic voting machines are any more secure. (2) *Since the machines do not produce a voter-verifiable paper ballot, if an attack is mounted or if something goes wrong with the voting machines, there will be no way to confidently perform a recount of the voters' original intents*.

¹ URL: <http://www.cse.ucsd.edu/users/tkohno>. Email: tkohno@cs.ucsd.edu.

² Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin, Dan S. Wallach. Analysis of an Electronic Voting System. In *2004 IEEE Symposium on Security and Privacy*, pages 27-40, May 2004. Originally published as Johns Hopkins University Information Security Institute Technical Report TR-2003-19, July 23, 2003. Available online at <http://www.cse.ucsd.edu/users/tkohno/papers/eVoting/>.

Our work catalyzed a national debate on electronic voting security. I come here to explain why I, as a computer security expert, am opposed to the use of existing paperless electronic voting machines in government elections. I will also discuss proposed strategies for improving the security of electronic voting machines. Although not part of my testimony, in the question-and-answer period I would be more than happy to address some of the unsound arguments about the security of existing electronic voting machines and certification processes that you may have heard in the past, such as the assumption that logic and accuracy tests can identify security problems, or the claim that because there have been no documented attacks against electronic voting machines in the past, the concerns of computer security experts must be exaggerated.

Classifying electronic voting machines: Existing systems versus the future/potential

The first thing that we must do is clarify *what types of electronic voting machines we are talking about*. Are we talking about existing, conventional paperless electronic voting machines, like Diebold's AccuVote-TS, and their near-future descendants? Or are we talking about currently hypothetical, conventional-style paperless electronic voting machines of the (probably distant) future? (Or are we talking about non-conventional, cryptography-based voting machines?) Many people don't make a distinction, and lump all electronic voting machines into the same pile, but that is a mistake.

I am going to talk about current electronic voting machines, and their near-future descendants, because I believe that it is those machines that are most relevant to this hearing. I am not ruling out the possibility of having "secure enough" and "transparent enough" conventional-style paperless electronic voting machines in the far future (I say "secure enough" because there is no such thing as absolute security), but creating such machines will require an immense investment in terms of time and money and research, not to mention the challenge of defining what "secure enough" means. We don't have such machines now. And we won't have them by November.

We cannot expect to have secure paperless electronic voting machines by November

Let me elaborate. We know that the AccuVote-TS system has many security problems. And because of the flaws with the current certification processes, we have no reason to believe that other existing electronic voting machines are any better. Although one might try to address all known security problems, either by patching the software or instituting new procedures, this is not sufficient to guarantee that the resulting system is actually secure enough for use in an actual election. There are several reasons why this is true.

First, *spot-treating security problems in electronic voting machines is like spot-treating termites, you can never be sure that you've gotten rid of them all*. This is especially true since those analyzing the security of a system are often contracted only for a limited period of time, and in that time the security analysts may only be able to uncover the most obvious security problems. Fixing those problems may "raise the bar" for an attack, but does not mean that there aren't other serious attack vectors for an attacker to exploit. (Of course, I should stress that security problems in voting machines are much worse

than termites in houses; this is because security problems can be exploited by intelligent, coordinated, and malicious adversaries, whereas termites are simply hungry.)

Second, *unless all components of the revised system, including the software and revised procedures, are open to the public for public scrutiny and review, the public will have no reason to believe that the spot-treatment actually succeeded in addressing the security problems.* This is illustrated beautifully by the evolution of the Diebold AccuVote-TS system. After my colleagues and I released our original analysis of the AccuVote-TS system, the state of Maryland hired SAIC,³ and then later RABA,⁴ to perform independent analyses of recent versions of the AccuVote-TS system. We and SAIC identified problems with the way that the AccuVote-TS voting terminals communicate with the back-end tabulation system. Diebold tried to fix those problems by incorporating cryptographic mechanisms into their system. But RABA found that Diebold's revised system had its own security problems (in their attempted fix, Diebold used the SSL cryptographic protocol, but without host authentication). *If Maryland had not commissioned RABA to conduct a subsequent analysis of Diebold's purported fixes to ours and SAIC's reports, no one, except for maybe an attacker, would have uncovered Diebold's insufficient fix to the problems we identified.* This begs the question: for systems that the public cannot openly inspect, when can the public be satisfied that security problems have been successfully addressed?

One popular recommendation is to institute new election procedures in an effort to fix technical problems with the security of paperless electronic voting machines. The above points also apply here since there may be additional security problems not addressed by the new procedures, and since there is no guarantee that the new procedures will be appropriately designed. But there is another problem with relying too heavily on procedures. In security we desire what is called defense-in-depth, which means that a system should remain secure even if one of its components fails. Unfortunately, procedures may not always be implemented correctly – i.e., they may fail. They may fail because the people implementing those procedures are malicious. And they may fail because someone implementing the procedures accidentally makes a mistake. At a recent off-the-record KSG/NSF symposium on electronic voting, an election official made the following observation: At a company, it is natural for new employees to make mistakes on their first day of work. This is problematic since, for elections, every election day is the first (and only) day of work for many, many people.

What can be done between now and November

Since spot-treating security problems cannot be expected to yield a secure enough and transparent enough system, what can we do with existing paperless electronic voting machines? Computer security experts, including myself, advocate adding a voter-verifiable paper ballot to existing paperless electronic voting machines. That is, retrofit

³ Science Applications International Corporation. Risk Assessment Report: Diebold AccuVote-TS Voting System and Processes, September 2003. Available online at <http://www.dbm.maryland.gov/SBE>.

⁴ RABA Innovative Solution Cell. Trusted Agent Report: Diebold AccuVote-TS Voting System, January 2004. Available online at http://www.raba.com/press/TA_Report_AccuVote.pdf.

Biography

Tadayoshi Kohno is a cryptography and computer security expert, a Department of Defense NDSEG Fellow, and an IBM PhD Fellow with the Department of Computer Science and Engineering at the University of California San Diego. Prior to joining the University of California for doctoral studies, Kohno was a cryptography and computer security expert with two of the nation's top computer security firms, Counterpane Labs and Cigital. Kohno has provided security analyses for and guidance to a wide variety of organizations, ranging from billion-dollar corporations like American Express and VISA, to innovative new technology startups. Kohno has over fifteen refereed publications in computer science and computer security, and has won multiple awards for his research.

The CHAIRMAN. Dr. Shamos.

STATEMENT OF MICHAEL I. SHAMOS

Mr. SHAMOS. Mr. Chairman and members of the committee, my name is Michael Shamos. I have been a faculty member in the School of Computer Science at Carnegie Mellon University in Pittsburgh since 1975. I am an attorney admitted to practice in Pennsylvania and before the U.S. Patent and Trademark Office.

From 1980 to 2000, I was statutory examiner of computerized voting systems for the Commonwealth of Pennsylvania. From 1987 until 2000, I was statutory examiner of computerized voting systems for the State of Texas. During those 20 years, I examined over 100 different voting systems. These were used to count over 11 percent of the popular vote in the United States during the 2000 election.

I view electronic voting as primarily an engineering problem to be solved through traditional scientific methods. Once standards are set for the degree and type of risk we are willing to accept in such systems, engineers can determine whether a particular system meets those standards. The tolerable risk can never be reduced to zero. No system of any kind ever developed for any purpose has been completely free of risk. The issue is not to eliminate it but to quantify and control it. It may be a difficult pill for the voters of the United States to swallow, but it is true nonetheless and always will be that some votes are lost, miscounted or never are cast in every election and this will always be so.

There are many types of DRE machines, and it is incorrect to lump them together in a single category. DRE voting is not new. It has been used in the United States for over 25 years and has been successful, though not perfect, during that time. Many brands of DRE systems have exhibited problems, including failure to start, freezing up during voting, displaying incorrect candidate names. Some possess identified security weaknesses, such as according the wrongdoer the opportunity to vote more than once during an election.

Of course, machines that do not work and are not suitable for use in an election should not be used in an election, but this country has no systematic process by which such machines can be pinpointed and kept from the polling place. We need one. Voting machines, like every other machine we rely on in society can be tested to determine whether they are reliable. We need such procedures.

A completely different sort of allegation that is made against DRE machines is they can be tampered with undetectably or may contain malicious software that no testing procedure or examination would ever reveal. Even the venerable New York Times declared erroneously on April 24 of this year that, quote, it is not hard to program a computer to steal an election. It is very hard. In fact, there has never been a verified incident in which a DRE machine was manipulated to alter the outcome of an election. DRE opponents respond, how do you know? Maybe the alteration was done so well that we will never find out. That response is completely unscientific. It asks us to believe that which has never been seen and which by hypothesis can never be seen. It is a pure article

of faith, which every person is free to accept or reject, but it cannot serve as the basis for logical debate.

I have asked DRE opponents exactly how they would modify a machine to influence an election without being detected. This of course must be done in such a way that the machine passes all tests with flying colors, yet performs its dirty work only during the actual election and, furthermore, does so in a way that leaves no trace and does not raise undue suspicion, given the political demographic of a particular precinct or jurisdiction. In short, it would be the perfect crime. No one has ever come close to giving a credible method by which this could be done.

When challenged, the response of the opponents is to say, we are not obliged to show you how to do it. You have to prove that it can't be done.

That is not the law. The various States require voting systems be safe for use, accurate and resistant to tampering. None of the requirements is absolute, and they require judgments to be made by responsible officials and bodies. Administrative action is never required to be accompanied by a proof that the action is perfect. If there were such a requirement, then government would grind to a halt.

The proposal has been made that the variety of problems exhibited by DRE machines can be solved by adding a device that will print out a piece of paper containing the voter's choices so she may verify that they correspond to her desired selection. If anything goes wrong, the voter has the chance to try again before her vote is officially cast. If all is well, the piece of paper is dropped or deposited into a box inside the machine. This proposal is embodied in several bills before Congress and at least one that is currently before this committee, Representative Holt's bill, H.R. 2239.

The argument goes that we receive paper receipts when we buy things, use an ATM machine or play the lottery, so why should voting be any different? The answer is simple. In commercial transactions, the paper is simply a piece of evidence. It is not an incontestable, self-proving document. Even a lottery ticket will not be awarded a prize if it does not match the electronic records of the central lottery computer. The H.R. 2239 proposal is to make the paper records supreme, something that we do not do in the commercial world.

If paper were in any way safer than electronic methods, then the whole bill might make sense. But it is not safer or better. This is a case in which the cure is worse than the disease. This country has a long and sorry history of vote tampering involving paper ballots. Since 1852, the New York Times has published over 4,000 articles detailing numerous methods of altering results of elections through physical manipulation of paper ballots. On average, one article has appeared in the Times every 12 days since it began publishing in 1851. Mechanical and electronic voting machines were introduced specifically to eliminate this problem. Any proposal to make paper ballots official once again ignores history and therefore dooms us to repeat it.

Adding a paper trail that can be viewed by the voters solves one problem and one problem only. It assures the voter that her choices were correctly noticed by the machine. It provides no guarantee

that the vote was counted or ever will be counted correctly or the paper viewed by the voter will even be in existence at the time a recount is conducted. And the paper trail surely does nothing to increase the reliability of a voting machine. If a device won't start on Election Day, then adding a printer does not increase its chances of working.

Paper trail proponents have not bothered to list the problems with DRE machines in an attempt to explain how the paper trail would solve them because they cannot do so. They have not explained why the paper trail would not be vulnerable to well-known and well-documented methods of tampering the paper ballots, for they cannot do so. All of the problems with DRE machines have solutions. None of the solutions requires a paper trail. I have given specific alternatives in my rather lengthy testimony, and I thank you for the opportunity to speak today.

The CHAIRMAN. We will accept the gentleman's testimony as all other individuals appearing here today for the record. Very frankly, fascinating testimony by I think all four of you.

[The statement of Mr. Shamos follows:]

**Testimony of Michael I. Shamos
Before the U.S. House of Representatives Committee on House Administration
July 7, 2004**

Mr. Chairman: My name is Michael Shamos. I have been a faculty member in the School of Computer Science at Carnegie Mellon University in Pittsburgh since 1975. I am also an attorney admitted to practice in Pennsylvania and before the United States Patent and Trademark Office. From 1980-2000 I was statutory examiner of electronic voting systems for both Pennsylvania and Texas and participated in every voting system examination held in those states during those 20 years. In all, I have examined over 100 different electronic voting systems, used to count over 11% of the popular vote of the United States in the 2000 election.

I view electronic voting as primarily an engineering problem to be solved through traditional scientific methods. Once standards are set for the degree and type of risk we are willing to accept in such systems, engineers can determine whether a particular system meets those standards. The tolerable risk can never be reduced to zero. No system of any kind ever developed for anything has been or could be completely free of risk. The issue is not to eliminate risk, but to quantify and control it. It may a difficult pill for the public to swallow that some votes are lost or miscounted in every election, but it is true nonetheless and always will be.

There are many types of DRE machines, and it is incorrect to lump them together into a single category. DRE voting is not new. Such machines were introduced in the United States in the late 1970s and have been successful, though not perfect, ever since. Many brands of DRE machines have exhibited problems, including failure to start, freezing up during voting, and displaying incorrect candidate names. Some possess identified security weaknesses, such as according a wrongdoer the opportunity to vote more than once or employing severely inadequate data protection mechanisms. Of course machines that do not work and are not suitable for use should not be used in elections. But this country has no systematic process by which such machines can be pinpointed and kept from the polling place. We need one. Voting machines, like every other machine we rely on in society, can be tested to determine whether they are reliable. We need such procedures.

A completely different sort of allegation made against DRE machines is that they can be tampered with undetectably or may contain malicious software that no testing procedure or examination would ever reveal. Even the venerable *New York Times* declared erroneously on April 24 of this year that "It is not hard to program a computer to steal an election." It is very hard; in fact there has never been a verified incident in which a DRE machine was manipulated to alter the outcome of an election. DRE opponents respond, "How do you know? Maybe it was done so well that we'll never find out." That response is completely unscientific. It asks us to believe that which has never been seen and which by hypothesis can never be seen. It is a pure article of faith, which every person is free to accept or reject, but it cannot serve as a basis for logical debate. I have asked DRE opponents exactly how they would modify a machine to influence an election without being detected. This of course must be done in such a way that the machine passes all tests with flying colors, yet performs its dirty work only during the actual election, and furthermore does so in a way that leaves no trace and does not raise undue suspicion given the political demographic of the particular precinct or jurisdiction. In short, it

would be the perfect crime. No one has even come close to giving a credible method by which this could be done. When challenged, the response of the opponents is to say, “We’re not obliged to show how to do it – you have to prove that it can’t be done.” But that is not the law. The various states require that voting systems be safe for use, accurate and resistant to tampering. None of the requirements is absolute, and they necessarily require judgments to be made by responsible bodies and officials. An administrative action is never required to be accompanied by a proof that the action is perfect and unassailable. If there were such a requirement then government would grind to a halt.

The proposal has been made that the variety of problems exhibited by DRE machines can all be solved by adding a device that will print out a piece of paper containing the voters choices so she may verify that they correspond to her desired selection. If anything goes wrong, the voter has the chance to try again before her vote is officially cast. If all is well, the piece of paper drops or is deposited into a box inside the machine. This proposal is embodied in several bills before Congress and in at least one that is currently before this Committee, Rep. Holt’s bill H.R. 2239. The argument goes that we receive paper receipts when we buy things, use an ATM machine, or play the lottery, so why should voting be any different? The answer is simple. In commercial transactions, the paper is simply a piece of evidence – it is not an incontestable self-proving document. Even a lottery ticket will not be awarded a prize if it does not match the electronic records of the central lottery computer. The Holt proposal is to make the paper record supreme, something we do not do in the commercial world.

If paper were in any way safer than electronic records, then the Holt bill might make sense. But it is not safer or better. This country has a long and sorry history of vote tampering involving paper ballots. Since 1852, the *New York Times* has published over 4000 articles detailing numerous methods of altering the results of elections through physical manipulation of ballots. On average, one such article has appeared in the *Times* every 12 days for the past 150 years. Mechanical and electronic voting machines were introduced specifically to eliminate this problem. Any proposal to make paper ballots official once again simply ignores history and therefore dooms us to repeat it.

Adding a paper trail that can be viewed by the voter solves one problem and one problem only. It assures the voter that her choices were correctly recognized by the machine. It provides no guarantee that the vote was counted or ever will be counted correctly, or that the paper viewed by the voter will even be in existence at the time a recount is conducted. And the paper trail surely does nothing to increase the reliability of a voting machine. If the device won’t start on Election Day, then adding a printer to it certainly does not increase its chances of working.

Paper trail proponents have not bothered to list the problems with DRE machines and attempt to explain how the paper trail would solve them, for they cannot do so. They have certainly not explained why the paper trail would not be vulnerable to well-known and well-documented methods of tampering with paper ballots, for they cannot do so. All of the problems with DRE machines have solutions, and none of the solutions requires a paper trail. Specific alternatives are suggested in my detailed written testimony. I thank you for the opportunity to appear before you today.

Paper v. Electronic Voting Records – An Assessment

Michael Ian Shamos¹
School of Computer Science
Carnegie Mellon University
April 2004

Abstract

There has been much discussion in the popular press concerning the use of contemporaneous paper trails to plug various perceived security risks in electronic voting. This paper examines whether the proposed paper solutions in fact provide any greater security than properly maintained electronic records. We conclude that DRE machines pose a number of security risks but that paper records do not address them. A number of alternatives to paper trails are suggested to respond to DRE security concerns.

1. Introduction

Among the arguments that have been advanced against the use of direct-recording electronic (DRE) voting systems are the following:

1. Voting machines are “black boxes” whose workings are opaque to the public and whose feedback to the voter is generated by the black boxes themselves. Therefore, whether or not they are operating properly cannot be independently verified and the machines should not be used.
2. No amount of code auditing can ever detect malicious or even innocently erroneous software. Therefore the machines should not be used.
3. No feasible test plan can ever exercise every possible combination of inputs to the machine or exercise every one of its logic paths. Therefore the machines should not be used.
4. Hackers can break into the FBI’s servers and deface its website. It ought to be child’s play for them to throw an election. Therefore the machines should not be used.
5. DRE machines have been plagued by a host of failures all around the country. Therefore the machines should not be used.
6. The DRE industry is dominated by a small number of companies, some of whose executives are announced supporters of the Republican party. An executive could command his programmers to add code to each machine manufactured by that company to move votes to a favored candidate, thus determining the outcome of the election. Therefore the machines should not be used.
7. Many prominent computer scientists have said that DRE machines cannot be trusted. Therefore they should not be used.
8. If added to a DRE machine, a voter-verified paper trail allows the voter to satisfy herself² that her voting preferences have been recognized correctly by the machine. Therefore, the voter-verified paper trail solves every one of the aforementioned problems and every DRE machine should be required to have one.

Each of these arguments will be examined in this paper and found fatally flawed, at least to the extent that it implies that machines cannot be relied upon to count votes in real elections. The numbered statements above all share the property that the first sentence of their premise is true, yet their consequent, that DRE machines should not be used, does not follow from the premise.

In 1993, I prepared a paper for the Computers, Freedom and Privacy '93 conference exploring the risks of electronic voting³. Since then, I have often been asked whether I still adhere to the opinions expressed in that paper in light of the incidence of widespread hacking, Internet worms and viruses, new cryptographic attacks and the increased use of DRE machines around the world. The answer is that I still hold those opinions but feel compelled to update the justification for them to respond to the arguments raised above.

Since the Industrial Revolution, man has chosen to rely on machines for tasks that are either impossible for humans to perform, or so expensive or repetitively boring that there is no justification for continuing to waste human labor on them. Many of these machines, such as cars, airplanes and therapeutic radiation equipment, among numerous others, have the capacity to take human life. They also commonly contain embedded computer systems. In the business world we rely on computers to execute financial transactions totaling at least \$2 trillion per day. It is well-known that all of these systems present risks. There are approximately 40,000 deaths annually in the U.S. due to automobiles⁴; some number of the victims are killed by malfunctioning software rather than human error. People have also been killed by the computer programs that control radiation machines⁵. In light of such failures, why do we continue to drive cars, fly on planes and receive radiation treatments? Why hasn't the government outlawed these killing machines?

The reason is that testing and safety procedures are in place that reduce the risks to levels that are deemed acceptable. There is no basis for applying different reasoning to voting machines. Once we decide what a tolerable risk in such systems might be, we can require that the equipment meet that standard. Perfection is never required, expected or even possible in any real system, though it is a laudable aspiration, and perfection is not required, expected or possible in voting systems, either. Federal Election Commission Standard 3.2.1 allows a maximum error rate of 1 in 500,000 voting positions⁶. With a typical ballot size of 235 positions, this is an allowed error of almost one in every 2000 ballots, or 0.2% of the vote.

When the safety procedures are found to have flaws, the flaws are ultimately corrected because of public pressure, government mandate or the relentless law of the marketplace. We are now seeing immense public pressure being put on voting machine manufacturers, along with threats to legislate, both of which are appropriate.

A secondary reason that machines presenting some risk of injury are not outlawed is that people generally have the option not to use a particular machine. This choice is also available to a voter, who may eschew voting machines completely and cast a paper absentee ballot.

While the United States has been using direct-recording electronic voting equipment for well over 20 years without a single verified incident of successful tampering, within the last year a number of people knowledgeable about computer security have questioned whether certain DRE systems in current use are sufficiently secure to be employed safely in elections. Some criticism of these systems resulted from examination of their source code, perceived flaws in their handling and use or from consideration of purely hypothetical scenarios. A calm observer

might take solace in the observation that if DREs are so dangerous, then surely at least one security hole would have manifested itself by this time. Realistically, however, hacking has been advancing at an alarming rate, and new attacks are constantly being discovered, so we are entitled only to a small bit of comfort from DRE history.

It is an error, though, to ascribe to DREs generally the bad attributes exhibited by some of them. The spectrum of available systems is broad. Some machines are excellent, some are terrible.

1.1. The “Black Box” Phenomenon

That a machine contains a computer and the computer contains object code not readily viewable or understandable by the public is by itself no reason not to use the machine. If it were, no one ought to own a personal computer. Neither passenger nor pilot can see or understand the software that operates the control surfaces of a jet plane. Such software could contain code, malicious or otherwise, that might send the plane into a dive at noon on a specific date from which the pilot could not recover. How do we know for a fact that such code is not present? We don't. Yet pilots and passengers continue to board planes every day. Let's look carefully at the reasons we allow jets to operate. All of them apply to voting systems as well.

1. It is beneficial to aircraft manufacturers to make safe planes. Planes that crash will not sell and will eventually be outlawed, not to speak of the legal liability associated with such incidents. This benefit induces the manufacturer to develop internal procedures designed, but not guaranteed, to produce safe products. It is beneficial to voting system vendors to make safe systems also. Whether they know how to do so, or have successfully implemented procedures for doing so, is somewhat questionable. In examining more than 100 different voting systems for certification purposes, I recommended that over 50% of them be denied certification. The quality and reliability of particular DREs is certainly a matter of concern, and later in this paper various solutions will be suggested.

I have heard it expressed that it might not be beneficial under certain circumstances for a voting system manufacturer to produce an honest machine, but that substantial gain could be achieved by distributing machines or software altered to cause the election of specific persons who may not actually be favored by the electorate. We will discuss below the practical difficulties with such a scheme, but if a manufacturer felt that its underhanded activities would not be discovered, such a fraud might be attempted despite the possibility of severe criminal penalties⁷. Therefore any plan for the administration and use of voting machines should contain safeguards against this type of manipulation.

2. Planes are built to high performance and engineering standards. Agreed. Voting machines, which are far simpler than airplanes, can be (but are not always) built to even higher performance and security standards.

3. Planes can be tested. So can voting machines. Neither needs to operate perfectly. Planes shouldn't crash much and neither should voting machines.

4. If a plane crashes, we'll know about it. The significance of this statement, made by DRE opponents, is that we would then at least be able to take remedial action to prevent a recurrence, a fact of little consolation to the victims' relatives. The argument is made that election can be stolen under our very noses and no one would be any the wiser. But that ignores the real political fact that elections are local and local party operatives have an extremely

accurate sense of how the community is going to vote. The smell of irregularity is sufficient to set off alarms resulting in investigations and recounts. DRE opponents claim erroneously that in a disputed election there is nothing useful left to recount since all the records that remain were made by the malfunctioning machine. But this argument is wrong because the software that was used in the machine survives. (We can deal later with the assertion that the software might modify or delete itself to evade discovery.)

5. The people who fly airplanes have a vested interest in their safety. The people who run voting systems are likewise committed to clean elections. Pilots have been known to crash planes deliberately and election officials have been known to manipulate votes. Safeguards need to be built in to prevent both of these efforts from succeeding.

In short, I am unable to discern any engineering difference that allows us to entrust our lives to aircraft but would impel us to avoid voting machines. Not to endorse questionable voting systems or trivialize the possibility of chicanery, but I believe I and the republic will survive if a president is elected who was not entitled to the office, but I will not survive if a software error causes my plane to go down.

1.2. Computer Security

It is pointless to discuss the security of a computer system in the absence of a well-articulated list of threats. So let's enumerate and deal with them in order.

1. Isolated attacks on individual machines. There are any number of ways of interfering with the operation of any computer system, such as pounding on it with a sledge hammer or the slightly more sophisticated technique of exposing it to several watts of radio-frequency emission. Such efforts fall into the class of mischief rather than tampering because they cannot be used to cause a predetermined result.

A different form of attack is to gain access the hardware or software of an individual machine or small number of such machines and alter them, either by connecting to ports and interfaces or by opening the machine by force or with the help of an insider who may have the keys, along with manuals, plans and source code listings for the machine. It should be obvious that no machines should be used that allows any voter to connect to it electrically to during an election and any device that permits this should be decertified immediately. The question is how to prevent people from modifying the machines offline or at least to be sure the tampering will be detected before the machines are used.

One solution is to ensure that all software needed to operate the machines, including the operating system, is not installed in the machine until election day. The authorized, certified software, distributed from a central authority (not the manufacturer), can be brought up at the time the polls are opened. In this way no advance modification of any software would be fruitful. If it is deemed undesirable to do a full machine boot, a portion of the code can be loaded on election day and verify through message digests and encrypted checksums that none of the prestored files has been altered.

2. Attacks by hackers or insiders at a polling place. The tendency to use networked voting machines at polling places for ease of administration also increases the risk that an insider could use a computer connected to the network to distribute malware to the voting machines after the election has begun. The miscreant would presumably remove the malicious code or restore the original at some time before the end of voting so that no trace would remain of the

misdeed. This sort of attack presupposes that the insider is able to erase evidence of his deed during the election, for if the altered software is still present in the machine at the close of polls it can be detected. It also is a highly localized manipulation that affects the results at a single precinct only.

3. Attacks by hackers or insiders at a central count facility. Now the magnitude of the problem grows because the number of votes that are potentially affected can be extremely large. There are 35 counties (out of a total of 3170) in the United States with populations exceeding 1 million⁸. The total population of these counties is over 73 million, approximately 25% of the country's population. A successful attack on central count systems in these 35 counties, (representing just 1.1% of the total number) would certainly influence any election, so every step must be taken to prevent such an event. Fortunately, in most states the results produced at central count stations are informational only, and are not the official election returns. With DRE systems, the ballot images representing individual voters' choices are stored both in the machine on which they were cast in redundant memories and also in removable modules than can be transported. All of these memories are cryptographically linked so substitutions and cracking are not feasible. A manipulation of the central count computer would not be to any avail since the totals produced there would not correspond to the canvass of individual precincts.

4. Insertion of malicious code by the machine manufacturer. There are two subcases. In the first, the manufacturer delivers software to a jurisdiction with prior knowledge of the ballot layout, candidate names, etc. for each precinct in the jurisdiction. The machine is programmed to behave perfectly before and after the election but to switch votes to favored candidates during the election. This manipulation is possible if the manufacturer is able to distribute software directly to specific precincts prior to an election. Countermeasures are discussed in sections 3.5 and 3.6, below.

In the second subcase, the manufacturer has no foreknowledge of the details of any specific election but distributes master software that causes candidates of a particular party to win in all future elections. The practical possibility of such a scheme is nil. There are about 170,000 election precincts in the United States. It is not possible to move a constant fraction of votes from one party to another in each jurisdiction without it being obvious that manipulation is going on because the political demographics of the precincts are too individualistic and distinctive. Therefore the software would have to be distributed with a database telling it how to alter the vote for each relevant candidate in each precinct. The database would have to contain at least the names of political parties and possibly candidates and would have to know in advance the precise hours during which all future elections are to be conducted so the machine would know when to behave properly.

This nightmare scenario, in which a small number of programmers manipulate the politics of the United States by injecting undetectable malicious software into voting machines has more in common with spy novels than it does with reality. For example, in the movie *Goldfinger* (1964), a crazed collector of gold apparently uses nerve gas to kill the entire garrison of troops guarding Fort Knox, then enters the vault where U.S. gold is stored and almost sets off an atomic device that would render the U.S. bullion supply radioactive and useless, which would immensely increase the value of his own holdings. When the film appeared, did the Army close Fort Knox out of fear that the plot was realistic? No. The reason is that adults eventually develop the ability to distinguish fact from fiction, a critical intellectual facility that should not

be abandoned simply because we are talking about voting. Did the Pentagon evaluate the plot to determine whether there were security weaknesses that ought to be remedied? Probably. Were some security procedures modified to reduce the probability that such a plot would succeed? Maybe. Is breaking into Fort Knox in such a manner absolutely impossible? No. Why, then, if there is some nonzero probability that a person could do it, do we allow our gold to remain stored there? It's because we never require perfection in real systems. We balance the risks rationally against the cost and other detriments of preventing the risks and make a reasoned determination. Just because a novelist (or a computer scientist) can dream up an entertaining doomsday plot involving voting machines does not mean we should toss them on the junk heap.

The argument I have with DRE opponents is that they insist that any conceivable risk of any kind of manipulation is unacceptable. That standard is never applied anywhere in human affairs, and there is no reason it should apply to voting, despite appeals to patriotism and pious claims that our very constitutional system is in jeopardy.

I do not propose that machines or software ought to be trusted just because they use advanced technology. In his 1984 Turing award lecture, entitled "Reflections on Trusting Trust," Ken Thompson demonstrated a method of hiding malware so it absolutely cannot be detected by any amount of examination of the corresponding C source code⁹. The technique involves corrupting the C compiler so that it recognizes certain patterns in the source program and compiles them into object code that performs not as written but as the malicious intruder intends. Of course if one is able to modify the compiler in this fashion the compiler could just substitute an entire program of its own choosing upon reading a "signal" string in the source text. Efforts to test the compiler to reveal its misbehavior would be frustrated unless one knew the signal string, since if the string were missing the compiler would always perform properly. Theoretically this hack enables arbitrary amounts of code to be inserted into any program at the cost of introducing but a short sentinel string to tell the compiler to start its dirty business.

The Thompson Trojan horse is frequently cited by opponents of electronic voting¹⁰ as a reason not to rely on voting machines. No one has ever suggested a remotely practical manner in which the world's compilers could become corrupted, but let's assume there is some way of sneaking a rogue compiler into a huge number of computers. This ignores the fact that jurisdictions themselves do not compile voting software, and that even though the source code may not be revealing, the object code contains all the evidence necessary to detect the intrusion. A decompiler can be used to verify that the malware is not present and/or that the object code being used corresponds to the original object code.

The argument has even been made that Turing's proof of the undecidability of the Halting Problem has some applicability to DRE machines¹¹. The cited paper asks us to draw the conclusion that "Determining that software is free of bugs and security vulnerabilities is generally impossible." That statement is true only if the word "generally" is carefully defined. A correct version of the statement, but one unsuited to the opponents' purposes, is "There is no procedure that is always *guaranteed* to determine whether an arbitrary program is free of bugs and security vulnerabilities." The unsolvability of the halting problem does not imply that no program can be proven correct, nor does it imply that the halting problem for restricted programs is unsolvable. For example, FOR-loops that do not modify the index variable or its limits and contain only straight-line code do halt. These are precisely the type of loops that are used for iteration in vote tabulation.

Assuming that one believes it is necessary for voting system vendors to produce mathematical proofs that their software is correct (an unreasonable proposition), one can easily imagine structuring a program that reads a finite number of ballot images and produces vote totals to be amenable to such a proof. I therefore must brand references to undecidability in the context of electronic voting simply as sophistry.

1.2.1. The Omniscient Hacker

Combining the misleading Halting Problem argument with the Ken Thompson code-hiding method produces a fantasy that I refer to as the “omniscient hacker,” which was explained to me by an opponent of DRE machines who will probably be grateful not to be named here. The hypothetical omniscient hacker is able to insert arbitrary amounts of malware into a voting system in such a way that it can never be detected by any amount of code reading (source or object) or testing (before, during or after the election), yet is able to alter the votes to achieve any predetermined result in any jurisdiction for an arbitrary numbers of years into the future. We need not yet go into the details of why such a thing is or is not possible, since a moment’s reflection reveals such a hypothesis to be no more than a purely religious belief. By the very premise of the statement the malware cannot be detected, so no amount of evidence of its non-existence can disprove the statement. If the malware ever is detected, the hacker will explain that he just didn’t do a good enough job hiding it, but he’ll succeed the next time. In this way belief in the omniscient hacker is indistinguishable from belief in a Supreme Being. There is simply no argument one can give that will dissuade a true believer, yet when the believer is asked for a demonstration he is unable to produce one.

That said, here is an adversary argument that demonstrates that the omniscient hacker cannot exist, though for the reason just stated I do not expect true believers to accept it. If we test the machine during the election by feeding it votes in a manner indistinguishable from regular voting, the malware must decide whether it is going to tell the truth or lie about the vote count. If it tells the truth, it has disabled itself and we need not be concerned that it is present. If it decides to lie, we will catch it, since we are casting a set of ballots whose totals are known.

It is of course possible that there are ballot combinations we may not have tried that will cause the malware to enter lying mode, but there is little risk that ordinary voters will happen upon those combinations either and the malware is either effectively silenced or it will be caught. One can imagine a magic input to the machine that will cause to begin lying (such as writing in the name “Turing” for President). But then activating this feature on every voting machine, or even a substantial number of them, would require a conspiracy of huge proportions.

By its very definition there can be no defense against the omniscient hacker, since we would never be able to tell whether he has been thwarted. (We might as well postulate the existence of an omniscient tamperer who is able to substitute an arbitrary number of voter-verified paper trails without detection. There’s no defense against him, either.) Belief in omniscience is a matter of faith. Those who really accept the possibility of an omniscient hacker will never be satisfied with DREs.

1.3. Voting Machine Standards

Since 1990, the Federal Election Commission has developed and promulgated Voting System Standards¹². The current version of these standards is now several hundred pages long.

They deal with hardware, software, telecommunications, security, qualification, testing and configuration management, among other issues. They are voluntary in that any state may, but is not required to, adopt the standards as part of its voting system certification process. As of this date, 36 states and the District of Columbia have done so. The standards are clearly a step in the right direction and obviously enjoy widespread state support, although one wonders whether the states have really evaluated the standards and found them to be meritorious or have adopted them for convenience. It is difficult, however, for a standards-making body to keep up with developments in computer security, develop countermeasures for newly-recognized threats and document them in the form of precise standards. Thus Volume I Standard 6.4.2, entitled “Protection Against Malicious Software” is just two sentences long: “Voting systems shall deploy protection against the many forms of threats to which they may be exposed such as file and macro viruses, worms, Trojan horses, and logic bombs. Vendors shall develop and document the procedures to be followed to ensure that such protection is maintained in a current status.” An Independent Testing Authority (ITA) would be justified in claiming that the standard gives no operational guidance in testing a system to see whether it is secure against malicious code. It also appears to pass the burden to vendors, who are the very parties against whom we seek protection.

Independently of the FEC Standards, Section 301 of HAVA¹³ purports to impose certain minimum standards on “each voting system used in an election for Federal Office.”¹⁴ The term “Federal Office” is not defined in the statute but the Department of Justice takes the position that it has the meaning defined for it in other Federal election statutes, namely, “the office of President or Vice President, or of Senator or Representative in, or Delegate or Resident Commissioner to, the Congress.” Laying aside for a moment the question whether Federal control of Federal elections is a good or bad thing, Section 301 of HAVA is unconstitutional on its face. While the Congress may make rules concerning elections for senators and representatives¹⁵, it has no power to specify standards for presidential elections. Article II, Sec. 1 of the U.S. Constitution reads in part: “Each State shall appoint, in such Manner as the Legislature thereof may direct, a Number of Electors, equal to the whole Number of Senators and Representatives to which the State may be entitled in the Congress . . . The Congress may determine the Time of chusing the Electors, and the Day on which they shall give their Votes; which Day shall be the same throughout the United States.” Thus Congress has no power to determine the manner in which presidential electors are chosen other than to specify the time and date of their election.

No one seems to have noticed this unconstitutionality, but more probably the states simply do not care, since HAVA allocates billions of dollars to them for acquisition of voting machines – a case of not acknowledging that the gift horse even has a mouth. In any case, HAVA does not deal at all with the problem of malicious software.

1.4. Testing

DRE opponents argue that DRE software may contain up to 50,000 lines of poorly-written code that is impossible to read or test¹⁶. The argument is misleading – deliberately so in the author’s opinion. It is true that complete voting software systems, including ballot setup and printing components, may reach that size, but the portions of code that accept input from the

voter and record ballot images – the very portions suspicions about which have given rise to calls for paper trails – are tiny by comparison.

While it is surely true that not every logic path of a computer program of any size can be exercised, this is obviously not a reason not to use software. Otherwise no commercial software would ever be used, and surely not in any situation in which human life were at risk. The issue is whether any combination of code reading, program testing, open source code publication and other techniques can give us adequate assurance that the software does not contain malicious code or logic errors that will cause votes to be altered. The answer is certainly yes. If code is too obscure, or contains portions that are not readily understandable, it should not be used. Only if the relevant programming is transparent and available to the public should we be confident about using it.

One should realize that the basic loop that interrogates portions of a touchscreen and interprets them as votes is not very complex, although an entire election administration system might be. When the user touches the screen the processor is notified through an interrupt and receives the geographic coordinates of the point that has been touched. A search is made to determine which box on the screen has been touched. Any code that is present that treats candidates differently based on their ballot positions should not be there.

1.5. Machine Failure

By far the most justifiable criticism of DRE machines is that they fail during service or in some cases cannot even be brought into service on election day. There are numerous documented instances of such failures. These incidents are real. They are intolerable when they interfere with the act of voting.

It is important, however, to understand the nature of the machines' failure modes. They do not suddenly decide to move votes from Democrats to Republicans. They may "hang up," refusing to accept any more votes. The mechanical components, particularly the touchscreens, may develop dead spots or fail to register at all. Switches and buttons wear out. Circuits exhibit erratic behavior. These situations can result in severe voter inconvenience and loss of confidence in the process. Long lines can develop, causing voters to balk and go home. The sight of technicians opening machines and replacing components in full view of the voters does not promote trust in the integrity of elections.

While voter inconvenience is certainly detrimental, the critical question is whether any votes are actually lost or modified when the machines fail. In properly designed DRE, no vote once cast is ever lost because ballot images are stored in redundant memories, including write-once devices. It is possible, however, for a machine to fail in such a way that votes cast subsequent to the failure are misrecorded. When the failure is discovered later, it may be too late to reconstruct the lost votes. This situation is akin to mechanical failure of a lever machine – regrettable, but not fatal so long as the failure is not systematic or deliberately induced.

The matter of machine reliability is a question of design, engineering, testing and adherence to maintenance procedures. The responsibility of the vendor is not to be overlooked. A proper voting machine procurement will impose heavy penalties on vendors whose machines do not conform to warranty. If a jurisdiction is unwilling to rely on indemnification by a vendor, a solution is to acquire spare machines and stand ready to deploy them as needed during an election.

It is the author's opinion that many of the so-called failures of DREs in fact resulted from inadequate training of poll workers in using the equipment. HAVA has created an incentive for counties to rush to procure and begin using DREs. Some jurisdictions have done so without adequate preparation, and have seen failures occur during an election. When machines are tested at the warehouse immediately prior to an election and are found to be working, yet cannot be started on election day morning, it is much more likely that the problem results from unfamiliarity with startup procedures than a sudden and unexplained failure of the equipment.

Despite energetic efforts by opponents to slow their adoption, DRE machines continue to be adopted at a prodigious rate. India, the world's largest democracy with over 650 million voters recently adopted DRE machines nationwide. Just its 600,000 villages constitute more than four times as many election districts as there are in the entire United States.

2. Paper Trails

It has been asserted that adding paper trails to DREs allows prompt detection of all of the possible intrusions discussed above. It is based on the mistaken belief that paper records are in some way more secure or free from tampering than electronic ones, which is not the case.

On March 20, 2004, a presidential election was held in Taiwan. The winner by 29,518 votes (out of over 13 million cast) was the incumbent, Chen Shui-bian. To achieve this result, the Central Election Commission had to declare 337,297 ballots as invalid, more than 11 times the supposed margin of victory. The voting method was by paper ballot, and there weren't even any DRE machines to blame. Surely if the voters could rely on the paper ballots to be counted properly this result could not have occurred.

2.1. Paper Records

Humans have a profound affinity for that which they can see and touch. This results in a deep reverence for the printed word, whether it is true or false, and explains the comfort people derive from paper receipts. There are very few paper documents that have preclusive legal effect, meaning that the writing on the face of the document is not subject to challenge.

There are basically four types of paper records:

1. Bearer instruments. Examples: currency, bearer bonds, checks, movie tickets. Here the instrument itself entitles the bearer to rights with no further inquiry into his bona fides. Title to the document passes with possession. These instruments are extremely convenient for transactions because they can convey rights and title instantaneously without resort to offline records and databases. They are also a frequent subject of theft.
2. Receipts. Instead of being a instrument used to effectuate a transaction, a receipt is merely evidence of the transaction. As such, a receipt takes its place among all of the other forms of evidence, including spoken words, videotapes, witness testimony, business records, computer databases, etc. The receipt confers no independent rights, but is given for several reasons. First, a party to the transaction usually insists on a receipt (a) as evidence of the transaction, as in an ATM withdrawal; (b) to verify the correctness of its details, as in a restaurant bill; (c) as an aide-memoire to recall the transaction. It is used in the event of a dispute to lend credence to the claim of one party or another. The contents of a receipt may be challenged or rebutted and the effect it has will be determined by the trier of fact.

3. **Business records.** These are notes kept by a business as part of its operations. Records kept in the ordinary course of business are admissible as evidence, but they are only evidence and may be challenged. They differ from receipts in that they are created by one party to a transaction and but are not normally reviewed for correctness by the other party. A dispute between a bank and its customer over a questioned ATM transaction usually turns on the question of which records are more credible, the customer's paper receipt or the bank's computerized business records.

4. **Ballots.** A ballot is an expression by a person indicating how she wishes to cast her vote. A ballot is a unique document defined by election law and is itself only evidence of how a voter wanted to vote. A ballot may be challenged on many grounds, including an allegation that the voter was not entitled to vote, the ballot was mismarked, the voter voted in the wrong precinct, the voter cast votes for candidates she was not entitled to vote for, the ballot was mangled, defaced or was otherwise unreadable. In many, but not all, states when the content of a ballot is disputed, a court is required to determine the intent of the voter in marking the ballot and is not bound by that the ballot actually says.

There are numerous other forms of paper records, such as documents of title, licenses, wills, diplomas, written offers, etc., that are not relevant to our discussion here. The question is what desirable properties, if any, do paper records have that would cause us to prefer them over electronic ones for voting.

The largest industry in the world in terms of daily cash flow is foreign currency trading, which often totals more than \$2 trillion per day. The entire world securities industry rarely exceeds one-tenth of that amount, and no sector that deals in physical goods can even approach it. The vast majority of foreign currency trades are made without any use of paper whatsoever, either in the form of an original order or a generated receipt. If computers are unsafe and hackers and well-placed insiders lurk behind every door, one wonders why the traders don't lose a billion dollars a day (or at least a million) as a result of malware. In December 2003, no less a figure than Senator Hilary Clinton stated while introducing her "Protecting American Democracy Act of 2003"¹⁷: "You go to an ATM, you get a receipt. You play the lottery, you get a ticket. Yet when you cast your vote, you get nothing. The systems used by the people of the United States to exercise their constitutional right to vote should be as reliable as the machines people depend on to get their money. What's required for money machines should be required for voting machines." Statements that play well to the electorate often fail when subjected to the cool light of logic.

Sen. Clinton is correct that Regulation E of the Federal Reserve Board¹⁸ requires a financial institution to make a receipt available when a consumer initiates an electronic funds transfer at an ATM. She might be surprised to learn how limited the legal effect of the receipt turns out to be. If a financial institution fails to provide a receipt through "inadvertent error," it is not in violation of Regulation E¹⁹. Furthermore, the receipt itself is only prima facie proof (subject to rebuttal) that the consumer made a payment to a third party²⁰. It is not proof of the amount of transfer and is of course of no effect at all in the case of an ATM deposit, since the data associated with the deposit is generated completely by the consumer, not the bank.

In the event of a later dispute between the consumer and the bank, the ATM receipt is evidence only and is not dispositive of the question what amount was transferred. The bank may challenge the data on the receipt based on its own records. Note that the receipt has been in the

hands of the consumer and thus has been subject to alteration or forgery, which means that the document itself cannot be given absolute effect. Of course in electronic banking transactions initiated over the Internet there are no paper receipts at all, yet this fact has not dampened enthusiasm for online banking.

The law governing ordinary sales transactions, the Uniform Commercial Code, gives no legal effect to receipts and certainly does not require them²¹. In fact, neither party to a sale transaction has the legal right to demand a receipt, although it may be a customary business practice to comply with such a demand.

Sen. Clinton would be positively dismayed to learn that a lottery ticket has even less value to its holder than an ATM receipt. State lottery rules typically provide that if a dispute arises between the holder of a lottery ticket and the state lottery bureau, the computer records of the lottery bureau govern. This New Hampshire Lottery rule is illustrative: “To be a valid ticket and eligible to receive a prize ... [t]he information appearing on the ticket shall correspond precisely with the Commission’s computer record.”²² The lottery rules clearly provide that computer records govern over paper ones.

And so it must be. If presentation of a small piece of paper were sufficient to claim a prize of \$363 million²³, the inducement to fraud and bribery to produce a counterfeit ticket would be extreme, and the nature of paper is that it would be essentially impossible to invalidate the ticket based on a physical examination because genuine ticket stock can easily be obtained. This raises the question what the purpose of a lottery ticket might be if not to ensure the buyer that he will get paid in the event of a win. Despite what the public might believe, the lottery ticket is simply a receipt, that is, an item of evidence that can be considered in the event of a dispute. It also provides the buyer with the opportunity, in the act of buying a ticket, to verify that the human operator typed in his numbers correctly. The issue is not that the lottery ticket machine may have malfunctioned, but that the human seller may have made a mistake. (As we have seen, if the lottery machine malfunctions, that is, communicates a different set of numbers to the lottery commission than those printed on the ticket, the buyer has no effective recourse.) Because the only human in the voting booth is the voter herself, and the voter has ample opportunity to review her ballot, the verification function of the lottery ticket is not relevant to elections.

The lottery ticket also serves to remind the buyer which numbers he chose so he can later compare his numbers with the winning ones. It is also necessary to claim the prize, since a lottery ticket is anonymous and transferable. The state must know whom to pay. None of these considerations is applicable to voting²⁴.

Of course Sen. Clinton’s Protecting American Democracy Act of 2003 is unconstitutional for exactly the same reason that Section 301 of HAVA is unconstitutional – it purports to allow Congress to legislate standards for presidential voting, a privilege reserved to the states.

When I raise the point to opponents of electronic voting that huge volumes of commerce are conducted based only on computer records, their answer is, “If anyone lost a billion dollars they would know. If someone steals votes, we’ll never know.” This explanation is appealing, but specious. If someone were able to manipulate a bank’s computer records to spirit away a huge sum of money, it is reasonable to believe that he could do so while at the same time not only deleting any computer records of the transaction but also modifying the bank’s records so it did *not* know there was any loss. But in any event it does not matter whether the bank knows

that it has lost a billion dollars or not – the money is gone and the risk the bank tried to avert has occurred anyway.

2.2. Electronic records

The areas of human endeavor in which electronic records are used in place of paper ones are far too numerous to list. Among them are banking transactions, income tax filings, medical diagnosis, military orders (including nuclear launch instructions) and securities purchases.

The public and the legal system have come to recognize that electronic records can be reliable if properly maintained. The Electronic Signatures in Global and National Electronic Commerce Act (“E-Sign”)²⁵ raises electronic records to at least equal dignity with paper ones. It provides that in “any transaction in or affecting interstate or foreign commerce ... a signature, contract, or other record relating to such transaction may not be denied legal effect, validity, or enforceability solely because it is in electronic form.”²⁶ There are a small number of exceptions for such specialized documents as wills and testamentary trusts and notices of termination of insurance benefits, but otherwise electronic records do not have inferior status.

The regulations implementing the E-Sign statute generally provide that electronic records are equivalent to those on paper²⁷. The Uniform Electronic Transactions Act (UETA) has been adopted in 45 states and is pending the three others. UETA specifies the legal effect of electronic records and has as one of its stated purposes “to promote public confidence in the validity, integrity and reliability of electronic commerce and governmental transactions.”²⁸ If electronic records are questionable in some way, how has this fact escaped the vast majority of our state and federal legislators?

The Federal Rules of Evidence give equal weight to electronic records in court proceedings as they do to paper ones²⁹. It is therefore a puzzle why electronic records should be acceptable for every other government purpose except voting. Neither E-Sign, UETA nor the Federal Rules of Evidence contain any receipt requirement.

2.3. Paper ballots

Paper ballots can be divided generally into those that are intended to be read and counted by humans, which we shall call Australian ballots to avoid ambiguity, and those intended to be counted by machine. The latter included punched-card and mark-sense (optical scan) ballots.

Every form of paper ballot that has ever been devised can and has been manipulated, in general with considerable ease. The reason is that humans are familiar with paper and its characteristics, how to mark it to look genuine and how to erase it. Likewise, the number of people in the U.S. capable of producing professional printed matter is huge. There are over 50,000 printing companies in the U.S., employing over 1.2 million people, of whom more than 100,000 are prepress operators³⁰. This means that it is not difficult to locate people who can print or modify documents.

Other types of manipulation, such as destroying ballots or substituting other ones, require no skill at all. By contrast, altering redundant encrypted write-once computer records is impossible even for experts. So assuming that the electronic voting records are written correctly in the first place (a subject that indeed deserves discussion), the possibility of modifying them later is remote.

The simplest form of paper ballot manipulation is ballot-box stuffing, that is, inserting extra ballots, usually genuine ones that have been pre-marked, into the container meant to hold only those voted by registered voters. In any jurisdiction in which the voter can touch a physical ballot and personally insert it into a ballot box, she can conceal extra ballots on her person and insert them at the same time. This is true whether the ballots are Australian, punched-card or mark-sense. The practice is so widespread that many states have statutes specifically dealing with the situation in which more ballots are found in the ballot box at the close of voting than the number of voters who appeared at the polls that day. The Florida statute is both horrifying and amusing: “[I]f the number of ballots exceeds the number of persons who voted, as may appear by the poll list kept by the clerk and by the stubs detached by the inspectors, the ballots shall be placed back into the box, and one of the inspectors shall publicly draw out and destroy unopened as many ballots as are equal to such excess.”³¹ Yes, ballots are chosen at random and discarded until the totals come out right! The most appalling thing about the law is not how the procedure is to be conducted, but that the situation occurs frequently enough that the law had to be drafted in the first place.

Actually, the Florida process solves nothing except to avoid the unseemliness of having more votes cast than voters, which is always an embarrassment. If the ballot box has been stuffed, the random discard process will not alter the candidates’ percentages on average. That is, whoever wins by the stuffed vote total will probably also win after the excess votes are tossed away, and the stuffers will have achieved their objective.

Another form of manipulation is to perform substitution of ballots on a large scale. In central-count jurisdictions, ballots are not counted at polling places but are transported by vehicle to a centralized counting station, usually at the county seat. The ballots are carried in transport cases outfitted with locks and seals, but the locks can easily be opened and the seals counterfeited. It can take several hours in large counties for the ballots to reach the counting station, giving ample opportunity for chicanery. Instances are known in which manipulators did not even bother to open and reseal the ballot cases, but merely substituted others that had been prepared once the total turnout in each precinct became known. This sort of manipulation is made easy by the fact that printed Australian ballots are insecure and transport cases and seals easily obtained from unauthorized sources.

One of the oldest and easiest forms of tampering is to invalidate an Australian ballot while touching it. When I was in middle school during the 1950s, our American history teacher explained that poll workers would break off a piece of pencil lead and insert it under their thumbnail. When they found a ballot voted for a candidate they didn’t like, they would make a second mark for some other candidate in the same office, thus creating an overvote that had the effect of erasing the undesirable choice. Once this has been done, there is no effective way to reconstruct the original ballot.

Because Australian ballots have to be marked and read by hand, there is no real prospect for tampering to occur on a national scale. The same is not true of punched-card and mark-sense ballots. The only remaining use of punched cards in the United States is for voting, and only two manufacturers remain in the business. Without giving a catalog of possible tampering methods, there are many parameters in card manufacture that can be varied to the advantage of one candidate or another if the voting positions corresponding to the candidates are known at the time of manufacture.

The problem of hanging chads, long known in the election industry, came to public attention in Florida in 2000. But for years many states used “chad teams,” groups of poll workers whose function was to tear loose chads from ballots before they were fed into the card reader. Once we allow a person to alter a ballot that has been cast by a voter, anything is possible. A perfect tool for punching out chads by hand is the metal tongue from an ordinary waistbelt. Small and easily concealed in the hand, it can be used the same way the old pencil lead was employed to overvote Australian ballots.

With mark-sense ballots it is known that if the areas for marking the ballots are printed improperly or the timing marks at the side of the ballot are skewed, votes that are cast will not be read properly by the scanning machine. More tampering is possible through the selective application of inks that appear white but absorb the infrared light that is used in the reading process. An answer, one might think, is that we always have the original ballots around to recount by hand, but mark-sense ballots are just as susceptible to loss, substitution or augmentation as Australian ones.

In general, the rampant problems with paper ballots are neither acknowledged nor addressed by opponents of electronic voting, who seem oblivious to the fact that their opposition to new technology, if successful, will compel us to retain something that is much worse.

2.4. The “Voter-Verified” Paper Trail

It is alleged that adding a so-called “voter-verified paper trail” to a DRE machine will either permit tampering to be detected or at the very least will provide a reliable record of how each voter voted that can be used for a recount, even if the recount must be conducted by hand. This is incorrect. A paper trail accomplishes one thing, and one thing only – it provides assurance to the voter that her vote was initially captured correctly by the machine. This is no small accomplishment, but it can be achieved in numerous other ways, as explained below. That is the only voter-verified part. The paper trail provides no assurance at all that her vote will ever be counted or will be counted correctly. The reason simply is that the paper trail itself becomes insecure at the moment of its creation.

First, if the machine cannot be trusted, which is the working hypothesis of paper trail proponents, then it cannot be trusted to deal with the paper trail safely. After the voter leaves the voting booth, it can mark her ballot as void and print a different one. The voter will have left the booth believing not only that her vote was cast and counted properly, but that it will also be counted properly in any recount. None of these beliefs is correct.

One might argue that inspection and testing of the machine would reveal such abjectly bad behavior, but the claim of DRE opponents is that no amount of inspection and testing is ever sufficient. If testing is adequate to reveal paper trail flaws, then it is adequate to uncover other faults in the machines.

Here is a further, but only partial, catalog of problems with paper trails.

1. The paper trail cannot be on a continuous roll of paper, since that would permit reconstruction of each voter’s ballot based on the order in which votes were cast. Therefore, the paper trail must consist of separate pieces of paper. However, once the pieces of paper are separated, the integrity of the trail is lost. Looking at a piece of paper, we will not be able to tell for certain where it came from. Stuffing and all other paper ballot tampering methods then become possible. The addition of cryptographic indicia, which has been proposed as a method to

prevent insertion of unauthorized ballots, cannot work since the voter will never know whether her real ballot contained the proper indicia when it was created. If it didn't, the ballot will not be tabulated during a recount.

2. Adding a paper printing device to a DRE machine naturally adds another component that can fail, run out of ink, jam or run out of paper. If DREs are alleged already to be prone to failure, adding a paper trail cannot improve that record. In Brazil in 2003, where a small number of precincts had installed paper trails, failure of the printers delayed voters by as much as 12 hours, a figure that would be catastrophic in the U.S.³²
3. There is no voter-verified paper trail machine that has been tested on any large scale.
4. States that propose to implement the paper trail have promulgated regulations stating that the paper shall govern over the electronic record in the event of discrepancy³³. This has the effect of making the insecure paper record paramount over the secure electronic one, a return to the early days of the Australian ballot.
5. With complex ballots, voters are prone to forget exactly whom they have voted for. When confronted with a paper record, they may erroneously claim that the machine made a mistake. This will call the machine's reliability into question, prompt calls for a recount and cast doubt even on machines that are functioning properly.
6. Paper trails do not address the problem of DRE failures. If the complaint is that a machine cannot be initialized for use on the morning of election day, then having a paper trail mechanism is of no help. In fact, the presence of the mechanism increases the load on the machine's power supply and processor and itself increases the probability of failure.
7. The paper trail requires a re-examination of meaning of the terms "ballot" and "official ballot." This is not a mere semantic exercise, but a question of great legal and, in some states, constitutional significance. Can a piece of paper be a ballot if it is neither marked nor touched by the voter? If so, significant statutory changes will be required. If the paper is the ballot, then what conceivable meaning can be ascribed to the computer count, which is not derived by counting the "ballots," but by processing the voters' original inputs that were separately used to generate the ballots? If the paper ballots are official, then we are put in the untenable position of having to certify an election without ever actually counting the ballots, unless an allegation of irregularity compels a "recount."
8. Each losing candidate will claim that the election was stolen from him by the machine and will insist that the only true indication of the voters' preferences reside on the paper, even if there is no evidence of irregularity or tampering. Thus paper recount will become the default method of vote counting, mitigated only by the high cost of such recounts. If this is to be the case, why use voting machines in the first place?
9. Paper trails cannot readily be viewed by disabled voters, requiring them yet again to reveal their votes to strangers in order to have them verified. It is no answer to say that there are other mechanisms to review their votes. If paper trail proponents truly believe the paper trail is necessary for fair elections, then elections will not be fair for the disabled.
10. A report of the Caltech-MIT Voting project concluded that the presence of paper trails actually decreases public confidence in the voting system³⁴. This can be understood as follows: would requiring airplane passengers to inspect the plane's engines before boarding enhance their belief in the safety of the aircraft?

My position on paper trails, despite their problems, is not an extreme one. If a manufacturer produced a reliable paper trail device and the remainder of his system were acceptable, I would see no problem in certifying such a machine. I am firmly opposed to any audit trail requirement, however, and even where audit trails are used, the paper record should never govern over the electronic one because it is vastly less secure. The proper use of audit trails is as evidence. If the paper trail totals differ from the electronic ones, that is the starting point for investigation, not the end of the issue.

3. Alternatives to Paper Trails

If paper trails are not the answer, are there practical alternatives that will not only render DREs safe but also persuade the public that they are safe? Let us assume that all of the security risks discussed above (except the omniscient hacker) are realistic. Are there measures other than paper trails that will prevent them? The author does not discount the importance of assuring the voter that the machine is working and that her preferences have been collected without error. This can be done in a multitude of ways that do not involve paper.

3.1. Audit devices

A prime motivation for audit trails is the possibility that the machine has been programmed improperly, either by accident or by design, or that rogue software has been substituted for the authorized version. Suppose we were to require voting machines to be architecturally separated into two distinct devices: a panel, possibly but not necessarily a touchscreen, whose only function is to display the ballot and capture voter choices, and a tabulation and recording device, which accepts input from the panel and performs computations. The panels and tabulation devices could be supplied by different manufacturers.

Now suppose we feed the output of the panel to two different devices simultaneously. One is the tabulation machine; the other is an audit device made by yet a third manufacturer and programmed by an independent body, such as an accounting firm or public interest group not affiliated with the tabulation manufacturer. The audit device displays the voter's choices on a screen of its own for verification. The voter views the audit screen, and if it is correct, presses a "VOTE" button. Both the tabulation device and the audit device make redundant read-only records of each ballot image. At the end of the election, all the records are compared. If they differ in any respect whatsoever, the results from that machine are called into question and an investigation is launched. An examination of the software installed in the two devices should reveal whose records are the reliable ones.

So long as there is no collusion between the audit device manufacturer and the tabulation manufacturer, no amount of tampering with either machine will go unremedied. The prospect of tampering identically with both, since their software systems would be completely different, is too small to consider seriously. The audit device could easily be outfitted so disabled voters could verify their votes.

3.2. Open source

The manufacturers of voting equipment claim that their software is a trade secret and go to extraordinary lengths to preserve that myth. The author has been looking at the source codes of voting systems for over 20 years and has yet to find any significant differences in their design

except possibly for the number of bugs they contain. They all do the same thing, albeit in somewhat different ways. No vendor's software is a significant selling point providing any competitive advantage over other systems – jurisdictions focus on the hardware. All the software has facilities for setting up elections, storing the candidate and party names in a database, presenting ballot choices to the voter, tabulating and storing the results and possibly transmitting them after the election. The systems vary in ease of use and capacity, but they do not contain trade secrets for the simple reason that every aspect of election setup and balloting is well-known to all.

One might speculate then on why they try to keep the source code confidential. The uncharitable view, which appears to have some justification, is that they don't want the public to see how bad their code is. A legitimate reason might be to avoid making matters easy for competitors, but that does not justify withholding information from the public that is necessary to promote confidence in the electoral process. Another reason is to hide security measures which, if disclosed, would provide a roadmap for hackers. I am somewhat sympathetic to that view, despite the meaningless but mocking phrase "security through obscurity," since I know a thief will have a much harder time stealing my car if he does not know where I have hidden the key than if he does, and a party who happens to find my hidden key will have no idea which car it fits.

On the other hand, there is no reason that the ballot setup, display, tabulation and reporting sections of voting system code should be kept secret, and manufacturers would be wise to accede to public demand in this regard.

3.3. Administrative procedures

The administrative procedures concerning the handling of DRE machines and materials are usually not spelled out at all, or, if spelled out, then not circulated and not followed. Many of the observed vulnerabilities in DRE systems stem not from problems of machine design, but from lax handling procedures. A thorough election administration manual should explain at least the following steps:

1. Custodianship of machines at all times, including transportation to and from polling places.
2. Receipt and registry of software to ensure that only authorized copies of everything, including operating system versions, are used in voting machines.
3. There should be no delivery of any software directly from vendors to jurisdictions; otherwise (2) will not be observed.
4. Deposit and security for ballot materials, including any election programming. Likewise, control of installation of election programming into voting machines.
5. Chain of custody for any removable media containing ballot images or vote totals.
6. In the event an audit trail is used, chain of custody for the paper ballot images.
7. Freezing of machines and their software at least until the election is certified and the time for any challenge has passed.
8. Exception procedures for handling irregularities during an election, including custody of partial totals on any machine that is removed from service.

3.4. Standards

It may not be fruitful to have all the states separately ponder and solve the myriad of problems in election administration posed by the sudden introduction of new voting technology. Knowledge and experience should be pooled and election officials ought to be able to rely on a full set of standards, including security and vote handling procedures, that they can follow. The FEC Standards were principally written for ITAs to follow, not for election jurisdictions, and do not specify processes that are responsive to numerous objections that have been raised to DRE voting.

The budget provided by HAVA is fully sufficient to fund development of a comprehensive set of standards and procedures which, if followed, would greatly diminish the number of problems observed at polling places.

3.5. Parallel testing

More than 15 years ago, in a Pennsylvania certification report, I wrote of the possibility that a DRE machine could contain an on-board clock and that an intruder could rig the machine so that it behaved perfectly in all pre- and post-election tests, but switched votes during an election. The prospect is even more real today than it was then, since computers now routinely possess such clocks. This attack presupposes that the software knows all dates and times for elections into the indefinite future, but let's assume it has such knowledge³⁵.

One solution is to forbid on-board clocks altogether, but that would limit various other capabilities, such as making a time-stamped record of happenings during the election. It also raises the question how one can tell whether a clock is present in a machine or not. The second obvious solution is to reset the machine's clock to a time on election day, run a test and then set the clock back to the correct time. This is ineffective since the machine could contain software that would detect such a change and know that it was being watched.

A better solution is to employ parallel testing, a plan originally suggested by this author that was used in 10 counties in California during the 2004 primaries. Under this method, a set of examiners is empowered to enter any polling place at the start of voting and commandeer any voting machine for test purposes. No actual voters cast votes on the selected machine. No change whatsoever is made to the test machine – it is not even moved from its position (to counter the argument that it might contain a motion sensor to warn that it was under test). The examiner votes a number of predetermined ballots comparable to the number that would be voted on a typical machine in that precinct. Of course, manual entry of votes by a human is an error-prone process, so a video camera is used to capture his actual vote entries. At the normal close of polls, the votes on the test machine are tabulated and compared with the expected totals. If any software is present that is switching or losing votes, it will be exposed.

The function of this test is limited. It of course does not ensure that even one other machine in the precinct is working properly. It is designed to detect the nightmare scenario in which some agent has tampered with every machine in the jurisdiction undetectably, a major risk cited by DRE opponents to justify the addition of paper trails.

The examiners would select precincts and machines at random on the morning of the election. It is an issue of statistical quality control exactly how many precincts should be chosen. This testing, while cumbersome, is much easier than statutorily mandated recounts in which a certain percentage of ballot images must be totaled manually.

3.6. Separation of candidate names

Perhaps the ultimate protection against malicious code is to keep candidate and party names segregated from the software so it cannot perform any meaningful manipulation. If the machine is programmed to move votes from one party to another, it will be stymied if it is unable to determine the party with which a candidate is affiliated or even which candidate is associated with a given ballot position. This can be done by presenting the candidate and party names and issue text in the form of graphic files that can only be read by a human being. The only thing the software can do is faithfully record the numbers of the ballot positions that were selected. Of course, since it also knows no candidate names, it can only report results by ballot position. To defeat such a countermeasure the software would have to contain a complete optical character recognition algorithm.

It is possible that in a conspiracy a tamperer's confederate could, while voting, provide information via touchscreen selections or the write-in panel that could inform the software of the particular voting positions to manipulate. However such an act would have local effect only, since it would take one confederate for each voting machine involved. It would not be feasible to perform manipulation on a large scale with such a scheme.

4. Answering the Objections

We are now equipped to respond to the objections to DRE voting raised in the Introduction.

Objection 1. DREs are black boxes. So are all other computer systems, on which we rely for our lives and our fortunes.

Objection 2. Code cannot be audited. Yes, it can. Not all code can be audited, and we can bar un-auditable code from being used in elections. We can also make the code available for scrutiny by an arbitrarily large audience by making source code open.

Objection 3. Machines cannot be tested. Why not? Every other type of machine can be tested, and voting machines are not nearly as complicated as airplanes.

Objection 4. Hackers can do anything. Only in books and movies. The hacking stories we read in the papers concern attacks over the Internet against systems that are deliberately held open for access by the general public. Voting machines, by contrast, are highly controlled and cannot be accessed over the Internet. Hackers are not omniscient and even vendors have trouble programming tabulation software correctly. The prospect that a hacker could not only manipulate an election but do it without exhibiting a detectable bug is so far-fetched an idea that no one has come close to showing how it might be done³⁶.

Objection 5. DREs are failing all over the place. The answer here is simple: buy reliable ones. The FEC Standards specify numerous tests designed to weed out unreliable hardware.

Objection 6. The vendor can rig the machines. But we can expose him through any number of mechanisms, including audit devices and parallel testing. And we can render his manipulations fruitless by separating candidate and party names from the capture and recording logic.

Objection 7. Computer scientists say DREs are unsafe. Since when was this technological issue to be decided by popular vote rather than by analysis? There are over one

million computer scientists and mathematicians in the United States³⁷. About 100 of them have signed a resolution in favor of paper trails proposed by www.verifiedvoting.org³⁸. No information is available on how many have any familiarity with the processes of voting or the actual architecture of DRE machines, but the total number represents about 1 in 10,000, a minuscule proportion. The good news seems to be that the other 9,999 out of 10,000 have remained open-minded on the subject.

Objection 8. Paper trails meet objections 1-7 and make DREs minimally acceptable. As we have seen, this is not true. The paper trail does no more than persuade the voter that her vote was initially captured properly, but at the risk of announcing to the voter that the whole process is so insecure that her own vigilance is necessary. If the voter has to be watching at the polling place, what sort of confidence will she have in the remaining procedures that are conducted outside her presence? We have shown a number of alternatives to paper trails that genuinely meet the objections raised.

DRE machines have been described, somewhat dramatically, as a threat to democracy³⁹. A far greater threat to democracy is a return to any form of paper ballot, but both of these pale in comparison to the fact, not widely known, that in each presidential election more than 5 million Americans who are eligible to vote and want to vote are unable to cast a ballot because they happen to be outside their home districts on election day and cannot comply with their state's absentee procedures. Many of these people are overseas. The claim that tens of thousands of Floridians were disenfranchised in the 2000 election because of butterfly ballots, though probably true, is insignificant when measured against the millions who were unable to obtain any ballot at all. If computer scientists are truly concerned about threats to democracy, that's one they should work on.

¹ The author is Distinguished Career Professor in the School of Computer Science at Carnegie Mellon University and an attorney admitted to practice in the Commonwealth of Pennsylvania and before the United States Patent and Trademark Office. From 1980-2000 he was statutory examiner of electronic voting systems for the Commonwealth of Pennsylvania. From 1987-2000 he was the designee of the Attorney General of Texas for voting system certification. During those years he personally examined more than 100 different computerized voting systems for certification purposes. In the 2000 election, machines for which he participated in certification (which did not include Florida) were used to count more than 11% of the popular vote of the United States. This paper was prepared to accompany the author's appearance on an electronic voting panel at the ACM Computers, Freedom & Privacy Conference held in Berkeley, California in April 2004.

² The feminine pronoun is used to drive home the fact that a majority of U.S. voters are women.

³ Shamos, Michael, "Computerized Voting – Evaluating the Threat." Proc. Third ACM Conf. on Computers, Freedom & Privacy. San Francisco, CA (Mar. 1993). Available at <http://www.cpsr.org/conferences/clp93/shamos.html>.

⁴ National Transportation Safety Board Publication NTSB/SR-02/02, "Safety Report: Transportation Safety Databases," September 11, 2002. Available at <http://www.nts.gov>.

⁵ Leveson, Nancy et al., "An Investigation of the Therac-25 Accidents," *IEEE Computer* 26, 7, pp. 18-41 (July 1993).

⁶ Available from the Federal Election Commission website at <http://www.fec.gov/pages/vssfinal/vss.html>.

⁷ N.Mex. Stat. Ann. 1-20-5 provides, "Unlawful opening of a voting machine consists of, without lawful authority, opening, unlocking, inspecting, tampering, resetting or adjusting a voting machine owned by any county, or conspiring with others to have the same done. Whoever commits unlawful opening of a voting machine is guilty of a fourth degree felony." In general, tampering is a felony but the penalties are probably not sufficiently high. *Quaere* whether under the New Mexico statute a manufacturer who ships rigged software would in fact be committing this crime, which seems to require modification of a machine after it has become owned by a county.

⁸ U.S. Bureau of the Census, "Population Estimates for the 100 Largest U.S. Counties: April 1, 2000 to July 1, 2002," available at <http://c2k0.census.gov/popest/data/counties/tables/CO-EST2002/CO-EST2002-09.php>. Six of the 35 counties are in New York; another six are in California.

⁹ Thompson, Ken, "Reflections on Trusting Trust," *CACM* 27, 8 pp. 761-763, August 1984.

¹⁰ Neumann, Peter, "Risks in Computerized Elections," *Inside Risks* 5, *CACM* 33, 11, p.170, November 1990

¹¹ Jefferson, David et al., "A Security Analysis of the Secure Electronic Voting and Registration System (SERVE)," Jan. 21, 2004. Available at <http://www.servesecurityreport.org/paper.pdf>.

¹² Available from the Federal Election Commission website at <http://www.fec.gov/pages/vssfinal/vss.html>.

¹³ There is one reference in HAVA to the FEC Standards, but it pertains to acceptable error rates in ballot counting.

¹⁴ 42 U.S.C. §15481(a)(5).

¹⁴ 42 U.S.C. §15481(a).

¹⁵ Article I, Sec. 4 of the U.S. Constitution provides: "The Times, Places and Manner of holding Elections for Senators and Representatives, shall be prescribed in each State by the Legislature thereof, but the Congress may at any time by Law make or alter such Regulations, except as to the Places of chusing Senators."

¹⁶ Bannet, John, "Hack-a-Vote: Security Issues with Electronic Voting Systems," *IEEE Security and Privacy Magazine*, Jan/Feb 2004.

¹⁷ Bill S. 1986, 108th Congress, First Session.

¹⁸ 12 C.F.R. §205.9.

¹⁹ 12 C.F.R. §205.17.

²⁰ 12 C.F.R. §205.17.

²¹ There is a type of document of title known as a "warehouse receipt," which is necessary for a buyer to secure possession of his goods in certain situations, that has special status under the Uniform Commercial Code. But this is not the sort of receipt one ordinarily receives from a merchant in a sale transaction.

²² New Hampshire Lottery Rule 7(C).

²³ The largest U.S. lottery payout in history, \$363 million, resulted from the May 9, 2000 drawing in The Big Game, a multistate lottery now known as "Mega Millions."

²⁴ In his CFP '93 paper the author endorsed the use of state lottery systems for voting (without giving receipts, of course) and still does because their security and reliability is proven daily all around the country and they are clearly trusted by the public.

²⁵ 15 U.S.C. §7001 ff.

²⁶ 15 U.S.C. §7001(a)(1).

²⁷ The Food and Drug Administration regulations are typical: "Where electronic signatures and their associated electronic records meet the requirements of this part, the agency will consider the electronic signatures to be equivalent to full handwritten signatures, initials, and other general signings as required by agency regulations, unless specifically excepted by regulation(s) effective on or after forth the criteria under which the agency considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper." 21 C.F.R. §11.1(c).

²⁸ UETA Comment 1(f).

²⁹ F.R.E. 1001 reads, "For purposes of this article the following definitions are applicable: (1) Writings and recordings. 'Writings' and 'recordings' consist of letters, words, or numbers, or their equivalent, set down by handwriting, typewriting, printing, photostating, photographing, magnetic impulse, mechanical or electronic recording, or other form of data compilation."

³⁰ Press release of the Indiana Business Modernization and Technology Corporation, Dec. 21, 2001.

³¹ Fla. Stat. §102.061.

³² Mira, Leslie, "For Brazil Voters, Machines Rule," *Wired News*, Jan. 24, 2004.

³³ Standard 2.1.1.4, "State of California DRAFT STANDARDS For Use of Accessible Voter Verified Paper Audit Trail Systems in Direct Recording Electronic (DRE) Voting Machines," Secretary of State of California, March 18, 2004.

³⁴ Selker, Ted. et al. "The SAVE System: Secure Architecture for Voting Electronically: Existing Technology, with Built-in Redundancy, Enables Reliability," CalTech/MIT Voting Project VTR Working Paper, Oct. 22, 2003, revised January 4, 2004.

³⁵ It is actually not difficult to deduce this information from the ballot programming, which usually contains the date of the election in a predefined text field, the presence of which could be required by the system.

³⁶ See note 16. Hack-a-Vote is a project in which students are asked to develop malicious vote-counting software and other students try to find the malicious portions. It's not easy when posed in that framework.

³⁷ According to the Bureau of Labor Statistics, in 1990 there were about 881,000 computer scientists and mathematicians in the U.S.

³⁸ Sparnaus, Edward, "Electronic Voting is Threat to the Constitution," *Executive Intelligence Review*, Jan. 30, 2004.

³⁹ Zetter, Kim, "How E-Voting Threatens Democracy." *Wired.com*, Jan. 29, 2004.

Biography of Michael I. Shamos

Michael I. Shamos is Distinguished Career Professor in the School of Computer Science at Carnegie Mellon University, where he serves as Co-Director of the Institute for eCommerce and a Director of the Center for Privacy Technology. He has been associated with Carnegie Mellon since 1975. He is Editor-in-Chief of the *Journal of Privacy Technology*.

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

From 1980-2000 he was statutory examiner of computerized voting systems for the Secretary of the Commonwealth of Pennsylvania. From 1987-2000 he was the Designee of the Attorney General of Texas for electronic voting certification. During that time he participated in every electronic voting examination conducted in those two states, involving over 100 different voting systems accounting for more than 11% of the popular vote of the United States in the 2000 election.

Dr. Shamos has been an expert witness in two recent lawsuits involving electronic voting: *Wexler v. Lepore* in Florida and *Benavidez v. Shelley* in California. He was the author in 1993 of "Electronic Voting — Evaluating the Threat" and in 2004 of "Paper v. Electronic Voting Records — An Assessment," both of which were presented at the ACM Conference on Computers, Freedom & Privacy. He has provided testimony on electronic voting to the Pennsylvania legislature and the U.S. House of Representatives Science Committee.

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

The CHAIRMAN. One point I would like to make. Historically speaking, any time there has been manipulation or suggested manipulation of a voting system, it has involved paper ballots. You basically suggested that the paper receipts will not, in fact, bring forth the security that their advocates promise. Do you have any details about what you believe would be the shortcomings of paper receipts in trying to resolve the DRE security-related issues?

Mr. SHAMOS. The issue with paper receipts and my problem with them is that there is no guaranteed chain of custody from the moment the voter looks at the piece of paper and says, yes, this is my vote. From that moment until the time that piece of paper has to be touched or reviewed by other people, there is no way of assuring that the pieces of paper have not been removed from the box, new pieces of paper have been added to the box, that the pieces of paper have not been altered, et cetera. And it is impractical with 1.4 million poll workers we have in this country, most of them volunteers, to have any kind of systematic system where we can ensure that from the time the voter sees the piece of paper until the time it is reviewed that nothing has happened to it. That is the problem we have had when there is a physical paper ballot of any kind, whether it is punched card or paper.

The CHAIRMAN. Dr. Rubin, the chairman of the EAC and other groups such as Brennan Center For Justice have issued recommendations for ensuring the security of the DREs, as you know. You are involved with the Brennan study, I am told.

Mr. RUBIN. I was asked to read, review it and comment on it, yes.

The CHAIRMAN. Do you have any further comments on that study or can you describe more about the security practices and how they protect the process?

Mr. RUBIN. I was asked to comment on this and then to participate in a press conference to publicly comment on it. Initially, I hesitated to do that, because I was worried about an endorsement of these recommendations appearing to—or being misconstrued to be an endorsement of paperless DREs. What in fact was intended was that, no matter what I say or anyone else says, there are people going to be voting on paperless DREs in November. And for those election officials, what advice can we offer? Rather than just saying everyone is in trouble, can we do something constructive? And under those assumptions, they came up with recommendations that I think are very good: hiring security reviews, setting up a group that would supervise the security reviews, some ideas for testing; and, you know, the recommendations are available for the public.

I think that while I would strongly advocate against using paperless DREs, I am not going to be naive enough to ignore the people that are using them. So I would recommend that those recommendations be followed in those cases.

The CHAIRMAN. Just one question. Probably not a perfect question for you, but does anybody here believe—that one should be able to take those with you out of the—

Mr. RUBIN. Take what?

The CHAIRMAN. A copy of the paper receipt with you out of the voting area.

Mr. RUBIN. Absolutely not. The problem with that is that two things could happen. One is you have the opportunity to sell your vote if you can show someone how you voted, and the other is you could be coerced to vote a certain way. The idea behind the paper is that you have some tangible record of how the person voted, but if you take it out of the polling place with you, you haven't actually voted.

Mr. SHAMOS. Mr. Chairman, there are systems in which the voter is given some form of receipt but that receipt cannot be used to prove how he voted. It is possible for him to verify that that particular ballot was actually counted in the election. In general, it is not possible to remove from the booth any piece of evidence that you would be able to use to prove how you voted.

The CHAIRMAN. Anybody else have any concerns still about the issue of your vote being secret? That is a huge issue or being able, frankly, to vote in secrecy. But out comes the paper—because, Dr. Shamos, you mentioned something interesting, a chain of custody. What happens with that? Dr. Rubin, would you like to respond?

Mr. RUBIN. I will say one thing about the secrecy. I believe it is the property of secrecy that makes this problem so hard. When we talked earlier about commercial transactions and all different kinds of transactions where we have paper, the difference between voting is that imagine trying to audit somebody's bank account without knowing which person performed which transaction. In an election, we have a secret ballot, and it is a privilege, and we decouple the voter from their vote. That makes auditing a lot harder than it is in any other application that we know because the very information we keep, which is logging who did what and when, you can't do in an election.

The CHAIRMAN. You can't go back and say that this ballot was John Smith or Susan Smith's ballot.

Mr. KOHNO. If I may extend comments. There are two main requirements of voting machines. One is that the result has the correct integrity, and the other is the privacy. And when people are talking about electronic voting machines, the focus has been—most people have been focusing on the integrity.

One of the results of our analysis is that with these electronic voting machines it could be the case where an election official or a poll worker—I am assuming that most of them are not malicious—but an election official or poll worker could look at the results, the files stored—the results filed on these Diebold terminals and figure out who voted for whom if they are watching the voting process all day. So I think that, you know, I wanted to throw that in as being another problem that I see with electronic voting.

Mr. WILLIAMS. Not true. The ballot files in that system are randomized. So even if you had your numbered list of voters and you knew the order that people voted, you couldn't correlate that to the ballots on the file. And even if they were, it wouldn't be a one-to-one correspondent because, although you may check into the polling place ahead of me, I might cast my ballot before you cast yours. So that is not going to be a one-to-one correspondent, regardless.

Mr. KOHNO. I think we are taking the discussion away from the main focus of this hearing, and we can talk about this off line. But I think that the important thing—you know, I don't want to focus

on Diebold, because, unfortunately for them, they are the ones that were publicly analyzed. There is a random serial number stored with the ballots when they were added and specifically for randomizing them for reporting at the end. But the problem is on the files themselves, they were stored in the order they were created. But I think, like I said, this is an issue that hasn't been seen very much; and the focus here I think is on preserving on the integrity.

Mr. WILLIAMS. The problem he is referring to has been changed. That was true of the version that they looked at. In the SAIC report in Maryland, one of their recommendations was that those files be randomized, and that has been done.

The CHAIRMAN. I think I not do disagree with you. I think it is appropriate—basically what you said is appropriate to the hearing. What the gentleman, Dr. Williams, answered is also appropriate.

Mr. WILLIAMS. The problem that secret ballot creates is that you cannot—the voter cannot verify their ballot. There is no way once the voter walks away from that voting booth that they can go back to that collection of ballots and pull out a ballot and say that is mine, because that would violate the secrecy of the ballot. The whole concept of a voter-verified ballot is questionable.

You say, what do we do in a recount? Let us look at lever machines for a minute. When you recount on a lever machine, there is nothing to recount. What you are doing is verifying that the machine is operating properly; and the assumption is that if the machine is operating properly, then the count is accurate. Same thing with the DRE machine. There is nothing to recount, and you are not technically doing a recount in the sense of a traditional recount. What you are doing is that you are verifying that this machine is operating properly. If the machine is operating properly, then the assumption is that the results are accurate.

Mr. RUBIN. I believe that DRE have managed to replicate the worse property of lever machines, which is that a meaningful recount is not possible. That is why I was never comfortable with lever machines. The nice thing about having the paper ballot, when it is time for a recount we know at the very least the thing that is being recounted was seen by the voter. We don't know the order.

The CHAIRMAN. On that point, I will let you finish.

Mr. RUBIN. The idea behind a meaningful recount is that the things that are being counted are ballots that were seen by the voters, and that is where the term voter verifiable comes in. I don't think it is important whether or not the voter can reach into the pile of ballots being recounted and verify theirs. They have to have some confidence in the procedures, just like they do in any election. But without those paper ballots existing, there is no hope of any recount; and I don't think the solution to hanging or pregnant chads is to throw away all the ballots.

The CHAIRMAN. I want to open this up to questions from other members, but you just made a point. The voter sees it, verifies, but how does the voter know it was counted? When you are dealing with paper, you could stuff a ballot box. Where is the chain of custody of the item? Who is watching all that? I mean, historically in this country, any problems we have had have been on the paper. If you are saying, wow, the voter gets this and there is my vote and I walk away, where did that paper ballot go?

Mr. RUBIN. I believe the chain of custody problem does not go away with electronic tallying. We should look at constantly improving the security and not deploying a system that is less secured than the one we had before.

The difference between lever machines and automated computerized machines is that software, if there is a problem with the software, either intentional or accidental—and anyone who has dealt with software knows the accidental ones happen all the time—that problem is in tens of thousands of machines. And when you program a lever machine, if you make a mistake, that is that one machine. And that is one of the differences between electronic systems and mechanical or paper systems, is that the problems are more localized.

The CHAIRMAN. If we are talking about rigging—that is what we are talking about—rigging an election either by manipulating paper ballots or by electronic manipulation, you would have to have the ability of someone to put a chip or something in every single machine and pull it back and put it in the next election and next election.

Mr. RUBIN. Not necessarily.

The CHAIRMAN. Because it is not like you can hack into these things.

Mr. RUBIN. The biggest concern that I have always had ever since our initial report came out is that the person writing the software who is putting together the machine, not that I think they are going to do something, but I think they are in a position to.

The CHAIRMAN. For a particular election. They would have to rewrite the software then.

Mr. RUBIN. Not necessarily. Perhaps they favor a particular party.

One thing I find, if we get mired in a particular attack, if I get asked, how would you attack a voting machine, and I come up with an answer for that. Then someone says yes, but we could put this procedure in place that would prevent it. For every single individual attack I may come up with, someone could have a counterargument, but it is hard to design a system that would inherently block all the different attacks one might be able to come up with.

I believe that the difficulty of analyzing software is one thing, and I have talked at length about that, but a bigger problem is the software isn't being analyzed. There is no way that the software in the Diebold machine that we analyzed was analyzed before it was deployed or they never would have deployed that system.

The CHAIRMAN. Was that system corrected?

Mr. RUBIN. I don't know, because they won't let me have a look at it. I believe—they claim that many of the problems that we found in the machines have been fixed, but I think, without public scrutiny, there is no way to know if that is true.

The CHAIRMAN. We went from not correcting the machines to an issue of paper ballots. I think some people are sincere in this. I think some people have made absolutely incredible statements that smack of politics. There are conspiracy theorists, people have done this for political purposes and are using this issue, while others are sincere on this issue. But I think the whole thing, frankly,

has gotten clouded because of one company or one statement. I just think it has gotten quite clouded. At least today I feel we are hearing a reasonable debate on some of the issues.

Mr. RUBIN. Let me rephrase the statement, which I think that if we have the capability of building voting systems where the vendor does not have an opportunity to rig it, that is better to do it than ones where they do have the opportunity, whether or not we think they are going to do it.

Mr. SHAMOS. Mr. Chairman, it is precisely the property of the software that is resident in all the machines that makes it feasible to test them. If someone plucks one machine out of a polling place and alters it, then unless we specifically test that machine we are not going to find the alteration. But if the vendor has inserted the alteration into every machine that it has manufactured, then we can use the same kinds of procedures that we use with airplanes and nuclear weapons and other systems that have the capability of killing people. We can use those analytical methods to test these machines and determine whether or not they have been altered.

The allegation is made, as I mentioned in my testimony, that no, no, there is no amount of testing that will ever reveal every flaw in the system. That is quite correct. We don't insist that every flaw in every system be found. We would never have systems if we insisted upon that.

Mr. KOHNO. If I may add to his comments, I think that—I guess I want the committee to be careful about analogies that are made. You find many people make analogies, “we do testing for airplanes and we do testing for cars,” et cetera. I think the important thing to keep in mind is, when you are testing these things, you don't plan to put them in an environment where there is someone actually trying to actively attack them. You can be flying in the air in a normal airplane and you want to make sure in turbulence that things will be okay, but for these voting systems there is an active attacker. This active attacker will try to not play by the rules. It is this that makes voting systems or security so difficult.

I just kind of wanted to point that out.

The CHAIRMAN. I understand that, but what makes the paper so much more secure? The State of Maryland, Ohio, Texas, any State, Georgia, they are smart enough in these States, and they don't want fraudulent elections—not one person wants fraudulent elections, but they are smart enough to randomly pull machines in and test them because someone, as you say, is trying to attack these systems. But they are smart enough to be able to do that.

But why all of a sudden is everyone saying the paper is so much more secure, when paper could be crumpled—once you look at your vote, it could be crumpled and thrown away. Fraudulent paper ballots could be stuffed in the ballot box. What makes you so convinced that the paper is so secure? Paper to me is 100 times more unsecure than any machine that we could randomly test, that the States could test.

Mr. KOHNO. I still think that the thing I tried to convey in my testimony was that paper still is not perfect. Paper can be crumpled, thrown away, all this stuff can happen to paper, but at least that is what we are used to now. We are not going backwards. The problem now is with electronic voting machines, like Professor

Rubin said, the public is not able to go in and analyze them and verify that the problems have actively been corrected.

The CHAIRMAN. The States could do that. Everybody in this room knows how to crumple a ballot up and toss it away or stuff a ballot box. Everybody in this room could be knowledgeable about that. I doubt maybe four, two or one of you could actually go in and be able to fix and manipulate those machines. You would have to have a conspiracy theory that they are sitting out there and manipulating these machines that we can't ever find out about.

Mr. RUBIN. As someone—I have been working with computers my entire career. One of the feelings that I have is that, one, something could go wrong and you just wouldn't know it. It might be easier to detect some number of missing ballots than some bits in a computer that were flipped. If you look at the system as a whole, if you look at the magnetic cards in the machines that have the tallies on them; and the thought that all of the votes are being kept in a medium that inherently has glitches and inherently has flaws and can often be undetectable, that makes me nervous. I will not say that paper is great, but, right now, I think computers are not ready for this important responsibility.

The CHAIRMAN. I think they could be.

I am going to move on to our ranking member. One question and I am going to move on, although this has been interesting I think for everybody. On that note, we don't know. Let's talk about something we do know, though, Dr. Williams, about the undervote in the elections. Wasn't there an amazing undervote when it came down to nonelectric machines?

Mr. WILLIAMS. In the 2000 election, Georgia had actually a higher percentage of undervotes than Florida. We sat there and watched the goings on in Florida and thought, wow, there but for a close election goes us. That, in fact, is what led us to switch to the DRE machines. With the DRE machines, we reduced our undervote at the top of the ticket from something over 4 percent to less than 1 percent, a factor of five.

The CHAIRMAN. The gentleman from Connecticut.

Mr. LARSON. Thank you very much, Mr. Chairman.

Let me also say I really appreciate this line of questioning, and I think the debate and the dialogue that is ensuing is oftentimes best between the participants which I would broadly categorize as individuals who believe in trust and verify and those that believe that scientifically and from an engineering perspective that we have to analyze the risk, then solve the problem.

I have an overarching question that deals with the practicality of implementation and a more technical question that deals with encryption and how that would coincide with Mr. Rubin's proposal. But my esteemed colleague, Rush Holt, who, as has been mentioned by several of you, is a proponent of the bill before us has asked me to ask these two questions; and I think they cut to the heart of what we are trying to get at. I am going to direct them at Dr. Shamos and Dr. Williams, but I would appreciate a response from Mr. Rubin and Mr. Kohno as well in the process.

Mr. Holt's question is, if a vote is a record of an intended preference of a voter, isn't a recount an attempt to revisit and recount the records of those intentions? If so, after a voter casts a secret

ballot on the electronic DRE machine and leaves the polling place and the polls close, is there any way, without a voter-verified audit record, that election officials or manufacturers or programmers can determine what was the intention of the voter? Is it possible to have a meaningful recount on a DRE? Question number one.

Question number two, which is a follow-up, what is the possibility that a problem in software, whether it be an inadvertent bug or a deliberate, malicious doctoring of software could go undetected?

Dr. Shamos, I will start with you.

Mr. SHAMOS. The first question was quite lengthy. I think I remember it. I actually dislike the phrase "meaningful recount" because I don't know what it means. The legal purpose of a recount is not to do a revote. The legal purpose of a recount is to ensure that the vote totals that were reported by the individual machines in the jurisdiction were correctly reported and correctly added up.

Mr. LARSON. Could you elaborate on that? Because I think this is a confusing item to a lot of people, the difference between a recount and a revote.

Mr. SHAMOS. Yes. We never use the phrase "revote" unless we are talking about holding the election all over again, but I think a lot of people believe that the word "recount" means that we go back and look at the original intention of the voter. That is generally not what is done in a recount, and that is not what is required by the State statutes for recounts.

The problem is, if you look at the procedure for vote totaling in this country, voting is exceptionally local. It occurs on individual machines in individual polling places. The number of precincts in the United States is over 170,000. The number of voting machines is much larger than that. We must take the individual totals from all of those machines and eventually gather them together into some central place where they are totaled for the entire Nation in the case of a Presidential election or in the county in the case of a sheriff's election.

The process by which the totals are transmitted to this central place is error prone. It is done by human beings, often writing numbers on a piece of paper. So what a recount consists of is going and looking at those totals to make sure that they have been added correctly.

Where there is a physical record in the case of, for example, a mark sense or optical scan ballot, it is possible to rerun the ballots through the machine, in effect creating what you would refer to as a recount, count them again and then report those totals. The problem is, if they have been counted twice, then which is the total that we really should be reporting?

In the case of mark sense machines, you can get some pretty reproducible results. In the case of punch cards, you can't take 10,000 punch card ballots, read them through a card reader twice and get the same results, because the process of actually reading the cards changes the cards.

In the case of the DRE machine, the way you assure that the vote that the voter saw before she left the voting booth is actually recorded, right now the process is you test the machine. We don't

test these machines enough. There aren't established procedures for doing it, but it is doable.

There are any number of ways of creating an additional record. For example, one could display the voter's choices on a screen, just as they are done now; and one could take a digital photograph using equipment not manufactured by the same voting machine vendor, take a digital photograph of exactly what was on the screen at the time the voter left the booth. That would constitute, if it were properly encrypted and stored, an unalterable audit trail of what went on in the voting booth.

There are many such solutions that don't involve the use of paper. It is not that I have anything against the wood pulp industry. It is that anytime you have a specific piece of paper that human beings can touch, it becomes losable, augmentable or alterable. When you have properly encrypted computer records, written in write ones memory so that nobody can change them, you don't have that problem.

The other question I think was with respect to software. How do we know that the software hasn't been altered? The same as we know with all other systems, we test them. That is the way we find out whether machines work or not.

Mr. LARSON. Would you agree with the New York Times or are you familiar with the New York Times article that they did recently comparing the testing of machines that occurs in Las Vegas in the gaming industry versus, say, our polling booths across the country?

Mr. SHAMOS. Yes, I am. I am very familiar with the New York Times article. I think they have had to add a new guy to the mail room to respond to my letters that I write to them.

I haven't agreed with anything the New York Times has said about voting during 2004 except that specific editorial to which you refer, and I agree with everything in it. The point was made there that the Nevada Gaming Commission carefully vets every software—every piece of software and every chip that goes into every slot machine in Las Vegas. It is essential for that huge industry for people to be able to rely on machines to pay off when you win, and it is essential that casinos—for them to not pay off when you lose. So there is a huge amount of money available to do this kind of vetting and testing. I agree that, if the money were available, precisely the same kind of thing should be done with voting machines.

Mr. LARSON. How much money would that require, in your estimation?

Mr. SHAMOS. I don't have an estimate.

Mr. LARSON. If the other panelists could respond.

Mr. WILLIAMS. We do a significant amount of testing in Georgia directed toward just exactly that thing. We get our software directly from the ITA. We do not get it from the vendor. So that we know that what we have is what the ITA qualified, not necessarily what the vendor would like for us to have. So we get the software directly from the vendor; and then, before it is ever used in the State, we run about 6 weeks of testing on it. Some of it is designed toward the use of the system, but some of it is designed toward se-

curity, to try to wake up any Trojan horses that might be present and things like that.

Once we are satisfied with the system, we freeze it, so to speak, and we take a digital signature of it, and the digital signature that we use is the exact same digital signature that NIST uses to validate law enforcement software. Then periodically, anytime that one of our staff is out in a county, they can run that signature against the county system and verify that that system has not been changed.

Mr. LARSON. Dr. Rubin.

Mr. RUBIN. I would like a chance to respond to your three questions, the last one being of the gambling example.

In terms of meaningful recounts, the important thing I think is the question, what happens when something goes wrong? Sometimes it is really visible. There was a case of hundreds of thousands of votes being tabulated by an electronic voting machine in a place where fewer people had actually voted. What do you do when something goes wrong?

Things go wrong all the time. I worked as an election judge in Baltimore County. At the end of the day, the totals that we got off the machine did not match the totals that came in the door. It was one or two people. So we got out all the books and we got out all cards and we sat there for about an hour and a half and counted everything up until we found the error.

What do you do if something goes wrong inside a DRE? You get a result that doesn't make sense. There is nothing you can do. But if you have a voter-verified paper ballot trail, a box full of paper ballots, you can at least count them. You have some recourse for something to do if something goes wrong.

That is my response to the first question.

The second one, I have a very simple answer. I do not believe that it is possible to detect malicious code when it is hidden well inside of other code. I have done experiments with that, with 40 graduate students hiding code and then trying to find code. It is just an intuition. I don't have scientific proof, but I find that when I travel to computer science conferences and the only thing they want me to talk about these days is electronic voting, when the topic of hiding code comes up, that seems to be the consensus that I find, is that it is much, much easier to hide code than it is to find it.

Finally, the question about the editorial about the gambling machines and the Gaming Commission. I don't know if you are familiar with the case of Rob Harris who worked for the Nevada Gaming Board. He was one of the testers of the slot machines. He wrote some malicious code that he put on a testing device which would download to one of the slot machines and then somebody could come in and put in a particular sequence of coins into that machine, it would turn it into a winning machine for a while. So his conspirators would go around and play those machines and win a lot of money. The way he got caught was that one of his relatives won a big slot and didn't have an ID on him, so the security escorted him back to his room where Rob Harris was in his room, and they started investigating. But they didn't catch it any other way.

The point I am making is that insider threat happens. Even with all the stringent controls on the gambling machines, he was getting away with that for a long time and would not have been caught if he hadn't have been careless.

I think the insider threat in anything electronic will be caught through some out-of-band mechanism like not having your ID, but there is nothing inherent about software that makes it easy to catch these things.

Mr. LARSON. Dr. Shamos mentioned encryption. We heard testimony in previous committee hearings as well about that being the way to go. What you talked about earlier seemed like a method of encryption, though I profess not to be either an attorney, a scientist or a physicist, but I am interested in that line of questioning and would ask if the panelists want to further respond to one another.

Mr. RUBIN. I would start off by saying that encryption is a valuable tool in the security arsenal. It has specific purposes, namely to hide information from an adversary, so governments use it to send information out to spies in the field. It is not something that can be blindly applied to a system to make it secure. You can't sprinkle encryption dust on a computer and make it secure. Encryption is a tool. When there is something that needs to be done to maintain confidentiality, you can encrypt it with a key, but then the problem reduces to protecting that key. So the biggest value of encryption is in taking a lot of information that you need to protect and reducing it to a small amount of information that you need to protect like a key which can then be put on a smart card or protected some other way. But, in and of itself, encryption is not going to give you secure voting.

Mr. KOHNO. I would also like to add to that in the fact—so encryption, like you said, is a specific tool, but I think lots of people confuse encryption with the science of cryptography. Cryptography is a much broader science with many different goals in mind.

I think one of the things that as a cryptographer I have seen often mistaken is that encryption provides—protects—if you take some data and you encrypt it, you protect both the privacy and the authenticity. That actually turns out not to be true.

I don't know how technical in the details you want me to get, but, essentially, if you talk to a cryptographer, encryption is the process of taking some message, applying a transformation to it, typically using a key. You get some ciphertext. The ciphertext—an adversary looking at the ciphertext will not be able to figure out what the original message was. So this might protect the privacy of the vote, assuming all the other things like key management are in place, but this doesn't mean that you can't actually controllably flip a number of bits.

The example that I might—by flipping bits, I mean change the contents of the message. So an example that I might give is that you have several different messages that you want to be sending: sequences of “yeses” or “noes.” You encrypt each of these individually. I take my message “yes,” I am going to encrypt it, take my message “no” and encrypt it, and take the next message “yes” and encrypt it, send these over separately. This doesn't prevent an adversary from taking the “yes” messages, preventing the delivery of

my messages and kind of shuffling the order of these messages I sent.

I am hoping that this analogy is getting across the fact that encryption doesn't provide authentication. It is a powerful tool in the arsenal, but isn't a be-all, end-all solution.

Mr. LARSON. Most of the testimony I have heard over the last couple of weeks really points out the complexity of the issue, that really when—the further you look into it and the more you peel away each layer of veneer, you find that there doesn't exist a true simple answer to this, and what the voters are looking for is a very simple solution. It seems to me, at least in listening to the testimony we have heard over the last several weeks, that it is a more complex issue. I tend to agree with Dr. Shamos, that I think we have got to analyze the risk and then come up with the best possible solution. I also would think that the four of you could probably get into a room and come out with a solution.

My question is, given the practicality of facing elections in November and wanting to assure the public, and this is a concern that the chairman raised and I think many people on the committee feel, we don't want the message to go out to the general public that their vote doesn't count or if they are voting on a specific machine that the machine might in fact alter the election in such a manner or have been altered in such a manner that their vote doesn't count. How do we, in the short period of time that we have, produce the best possible result?

Mr. SHAMOS. I can start with that one.

First, on the issue of can machines be tested adequately, I find myself in the rare position of agreeing with Dr. Rubin on a few points that he just made. It is true there are always going to be insider attacks. We will develop countermeasures, and some new insider will find a new and better attack the next time, and the battle never ends. It is notable that after the discovery of the Harris debacle in Nevada, they didn't stop the slot machines from spinning. You can still play the slots in Las Vegas, even though there was an insider attack. If we insist on perfection, if we insist on zero defect, there is never any kind of system we are ever going to be able to deploy.

With respect to what to do between now and November, the only answer at this point seems to be test, test, test and train, train, train. Many of the problems that have arisen with DRE machines can be ascribed to first-time use. Poll workers who have never seen the machines before were asked to follow procedures that didn't even exist in written form. So training is required there.

If it is believed that the security vulnerabilities in these machines can be exploited in order to alter the results of an election, then security measures must be taken to ensure that that doesn't happen. You don't leave the machines around, for example, where outsiders get an opportunity to play with them. You watch what people are doing when they are going into the polling place. I don't see any alternative to those two steps before November, which is, I believe, 120 days from now.

Mr. WILLIAMS. I agree with that.

To get back to the Brennan report that supposedly is recommendations for things to do for 2004, it can't be done. The

things that are in that report: to start today and go out and try to hire a consultant, bring that consultant in, evaluate your voting system, get the recommendations, implement those recommendations and hold an election 120 days from now, you can't do it. It is a catch-22 situation. If you try to do it, you are going to wind up running your election with an uncertified system, and you are going to get criticized for that. So if you don't do it you are going to get criticized for not doing it. So that Brennan report puts us in a real catch-22 type situation.

Mr. RUBIN. I believe that if there is a vulnerability out there, it is better to know it than not to know it. Hiring security consultants to come in and review the system and produce a report and if they find something, then at least you know about it and then we can figure out what to do about it. It is better than not knowing about it.

When we analyzed the Diebold system a year ago, it was a year and a half left until the election. We asked ourselves, will we do more damage or good by going public with this? One of the things we said, well, there is not an election coming up. We have a year and a half before the election, plenty of time to fix the things we are talking about and design perhaps and provide better voting systems. We did go public with it.

Right now, we are coming up to the election. We need to do everything we can. Unfortunately, I think there are places that are going to be used, equipment that I don't believe in, that I don't believe is secure enough. Should I sit back and say, well, in order to preserve the confidence of the voter in something I think is insecure, do I sit back and keep quiet? I don't think that is a good idea. That is why I have been speaking out about this.

Mr. LARSON. Would you agree with Dr. Shamos that what we should do then, given the shortness, is test, test, test? Is that a reasonable alternative?

Mr. RUBIN. I think that I do believe in parallel testing, and I believe we should maximize the testing but not in place of external review. I think you can test and review at the same time.

Mr. LARSON. The review that you are indicating would be the review that you laid out in your testimony?

Mr. RUBIN. No, the review that the Brennan Center and SSCR recommends in their recommendations that came out last week.

Mr. WILLIAMS. Which is based on the assumption that we don't already know the vulnerabilities in our voting system and we need somebody else to tell us about them, and we don't agree with that.

Mr. RUBIN. No, but that is one of the assumptions.

The CHAIRMAN. Mr. Mica.

Mr. MICA. Thank you, Mr. Chairman.

We have got a couple of experts that have looked at the overall picture here. What percentage of our voting will be done in 2004 by electronic means?

Mr. SHAMOS. It was estimated originally at about 32 percent. The estimates have been falling to somewhere in the 20s, which is somewhere between two and three times the percentage that voted under the early machines in the year 2000.

Mr. MICA. Basically, the machines that are out there, do any of them have a paper trail capacity?

Mr. SHAMOS. Many of them have a paper trail, one that is not viewed by the voter, however. Most DRE machines—at least when I was involved in certification, most DRE machines have an internal paper trail that records in random order a complete ballot image of every vote cast. In that sense, they have a paper trail.

Mr. RUBIN. That is not what the Diebold machines do, though. They print out the totals at the end of the day on a printer, but they only maintain an electronic total.

Mr. MICA. But that is an electronic total, not as everyone votes?

Mr. SHAMOS. It is as everyone votes. Not in Diebold.

Mr. MICA. It is just adding a number as opposed to sort of a continual tab on how each one has voted?

Mr. SHAMOS. Yes. I am in the enviable position of never having reviewed the Diebold system for certification purposes, so it can't be blamed on me.

Mr. RUBIN. These machines do not print anything throughout the day until the end of the day when they print totals. They do not print anything as people vote.

Mr. MICA. Then I heard the dilemma, if we have a discrepancy in a paper trail versus an electronic trail, how would that be resolved?

Mr. RUBIN. There isn't a paper trail in the Diebold machines.

Mr. WILLIAMS. That is not entirely true. As you know, the HAVA legislation requires that the system have the capability to print ballot images. The Diebold system can do that. As a matter of fact, it can print them in a format that can be read on an optical scan machine if you want to. I have never known anybody to actually do that, but the capability is there.

Mr. RUBIN. That would be a pretty useless thing to do.

Mr. MICA. Hey, join the club up here. We do a lot of useless things and spend a lot of money doing it, too. That is part of my point.

Okay, everyone has agreed that there is no way to verify the vote of an individual.

Mr. SHAMOS. With the current systems that are deployed, that is correct.

Mr. MICA. And we have no way of really changing—everyone agrees that before this election basically there is no way to add any other security checks or enhancements to existing machines, that what we have got is what we are going to go with, basically?

Mr. WILLIAMS. That is right. We talk about November, but November is not really the date. You have got to send out your absentee ballots 45 days ahead of time. So, actually, you have got to put your election to bed 45 days before November 2.

Mr. MICA. I am trying to get a glimpse of the 2004 election. I think you are providing that.

I don't mind spending Federal money to make certain that an election improves voter participation and accuracy and security. However, I am concerned the way we spent money here, I think we did it by a formula, and each State got, based on population of voters, a distribution. Is that the right way? What should the Federal role be in this process?

Traditionally, you heard my comments at the beginning, the State and locals really run the show, and you have got a mass—

someone said 1.4 million volunteers. These aren't people that we are taking in and giving computer technical training and operations. These are folks that will get a little course here and there.

To get the biggest bang for the Federal buck—and, also, what is our Federal responsibility in this process? Maybe we could go down—that will be a major question. What is our best role with our money and our position to make this work in a cost-effective manner and that gets us the best results?

Mr. SHAMOS. Until recently, I believed that the best role for Federal Government in elections was hands off. Unfortunately, what has happened is that the States' attitude has also been hands off. The States have one by one been abdicating their responsibility for testing and certifying voting systems. What they have done is to rely instead on the Independent Testing Authority process and the voluntary FEC standards, which are now known as the FVSS. The idea there is that there are some standards voluntarily proposed by a body and there are independent testing authorities who supposedly test the machines to those standards and they produce a letter that says—

Mr. MICA. When you say "machines," are you just talking about electronic? Or all machines?

Mr. SHAMOS. There is computerized voting and then there is DRE voting. I am including anything that involves a computer. The Independent Testing Authority produces a letter that says we tested this system to the Federal voting system standards and it passes. In many States, that is sufficient. The States themselves don't do any subsequent evaluation of the machine. They just accept that letter at face value.

It is obvious that there is something wrong with that process, because all of these systems that have been found to have security flaws, particularly the system examined by Dr. Rubin and his colleagues, they were all ITA certified. And so it raises the question exactly what are these ITAs doing and are the standards adequate.

I have looked at the standards. They are 300 pages long, and I have them with me. Many of the concerns we have discussed today received no attention or one or two sentences' worth of attention in these standards. So I don't believe the standards should be voluntary.

I think that in elections for Federal offices there should be mandated Federal standards these systems should have to obey, and there has to be some serious attention given to updating the standards and keeping them updated. As new attacks and new modes of attack are discovered, there have to be new standards to attempt to respond to those. We don't have such a system right now.

Mr. MICA. Anyone else?

Mr. WILLIAMS. We don't have the system, but you have put in place the mechanism. The EAC is the organization to address these problems. It has been slow getting off the ground, but with all of the problems that we know are in the HAVA legislation, I think basically it is doggone good legislation.

I have worked with the NASED program, the FEC program since its inception in 1986; and it has been an entire volunteer effort. That shows. With things that Mike is talking about here, there are problems with it. The problems are primarily—it is not because we

didn't know better. It is just because we didn't have the resources. But now with the HAVA legislation, we have got the resources.

The Technical Development Committee is meeting for the first time Friday. They have 9 months to produce a preliminary standard. Things are beginning to happen. I think the best thing that this committee can do right now is to give the HAVA legislation a chance to work.

Mr. SHAMOS. The problem I see there is, even after the EAC does its work, the standards that it develops or the standards that it developed under its leadership will still be completely voluntary standards. It will not be mandated for the States to follow.

Mr. WILLIAMS. Yes, but I would like to not say a priori that those are going to be the law. Let's develop them, look at them and decide whether or not they are good enough to be the law. Let's let people like sitting here at this table take a look at those standards.

Mr. MICA. You are saying the standards will be sort of an evolving set?

Mr. KOHNO. I would like to comment on that.

Someone made an argument to update the standards as we find new attack modes. That kind of hints at what concerns me most as a computer security expert. These machines are still new. The assumption is that we are going to expect to keep finding new attack modes. That I think is a very scary idea, because it means that we are at a state where we don't know what all the attacks are. We are going to be finding new ones and evolving the standards over time. I don't want to be using something that is standardized, and the standardization says this is what we know now, but it is not perfect. There might be attacks discovered in the future, so we are going to revise these standards.

But the first question you raised was along the lines what can the government do. I am a computer security person, not a person in the government. I don't know what is within the limitations of me to allow for you to legislate, et cetera. But I think that one thing I believe is very important is for the voting process to be very open.

I think Ranking Member Larson asked a question earlier or was talking about—there are two different issues going on. One is, are the elections themselves going to be secure? The other issue is, will the public believe that the elections are secure? I think these are two different things, and I believe one important thing we need to think about in the future, you have to weigh the importance of these two things. Do we want a system that is secure but the public doesn't have faith in for various reasons? To me, I believe it is important for the public to believe the election was secure. Toward this end, I believe developing a model where the public can look at and verify for themselves that the voting systems are secure and reliable is very important.

Mr. MICA. Dr. Rubin is the only one that didn't comment.

Mr. RUBIN. I think the best thing the Federal Government could do is put independent back into the Independent Testing Authority. They should be the ones hiring the testers and the certifiers, as opposed to the vendors who are making the machines.

Mr. MICA. Thank you.

The CHAIRMAN. The gentlewoman from California.

Ms. MILLENDER-MCDONALD. Thank you, Mr. Chairman. From the testimony this morning and if the public is looking and listening, they have absolutely validated that there is no assurance that there is security in their voting. This is what members in the minority community grapple with all the time, that their vote will not count because there is no verification that their vote is being counted. But the one thing I suppose we can all agree to, that there is no such thing as a risk-free system. Am I correct, gentlemen?

Mr. SHAMOS. Yes.

Ms. MILLENDER-MCDONALD. Secondly, whether there is a paper trail or not a paper trail, there is never a means for a complete or verification accuracy count, am I correct on that? Is that a correct assumption?

Mr. WILLIAMS. Not as long as we have secret ballots.

Mr. SHAMOS. In the currently deployed systems, that is correct. There are proposals for systems that would remedy that defect.

Ms. MILLENDER-MCDONALD. Let me ask you, for the umpteen years that I have voted—and I do not care to tell you those number of years—when you go to the polls to vote, you have a ballot that is given to you. The ballot has a top part that is detached from when you finish and complete your ballot, and they put that larger ballot into a box, and they give you this little detached piece saying that I have voted or whatever it says, but it carries a number. That number cannot be verified if there is a recount? You can never go into that box? Assumedly, that is the box you voted from—or is that the operative word? “assumedly,” that is the box you voted—your ballot went down in, to compare that from that stub that you get, compare it to the ballot that is put into the box?

Mr. SHAMOS. No, because the number is on the stub only. It is not on the ballot.

Ms. MILLENDER-MCDONALD. I see.

Mr. SHAMOS. It is a privacy problem.

Mr. WILLIAMS. In most States, by law you cannot have any identifying mark on the ballot that could be identified back to the voter.

Ms. MILLENDER-MCDONALD. In other words, then it is true that we do not—the position is not there or the system is not set up for recounting to be done accurately then? Is that a fair statement?

Mr. RUBIN. The idea behind the meaningful recount concept of voter-verifiable ballots is that if you have a box full of ballots that voters looked at and put them into that box, then while you won't know which ballot corresponds to which person, it is the best effort, best hope you have of counting the voter's intent.

Ms. MILLENDER-MCDONALD. Absolutely true.

Mr. RUBIN. That is why I and many others have been advocating voter-verifiable paper ballots, so that you have something to go back and count.

Ms. MILLENDER-MCDONALD. Yet we don't have to bring up Florida again. Because Florida indicated that, even with a paper ballot, that was not an assurance that that could be a count that was accurate in the sense of accuracy.

Mr. RUBIN. The ideological difference is that I think the way to improve Florida is to design better paper ballots where you won't have hanging chads or be confused about which hole to punch. You can accomplish that with a system I described in my initial testi-

mony where you have all the benefits of a DRE for vote casting but you have all the benefits of paper for vote counting.

Ms. MILLENDER-MCDONALD. Dr. Williams, in your testimony you indicate that you do have your DRE now in place for Georgia, the State of Georgia. It has been replaced by all other systems that you have once used.

Then I see an article by the California Secretary of State Shelley who says in this article, a number of failures, including touch screen machines in Georgia, Maryland and California, has spurred serious questioning of the technology. Of course, as you know, our Secretary of State has banned to some degree the use of the Diebold system, although in one of my cities in my district we do use it, and he has not banned that one. But he is kind of contradicting what you have said in your statement, or is that a contradiction?

Mr. WILLIAMS. I have no idea what he is talking about. We installed that system—we first used it in November of 2002, and we have right now held over 500 elections using that system, and we have not had a problem yet that we could attribute to the system per se. We have had problems, but they have all been typical human-type problems that you have with any system.

Ms. MILLENDER-MCDONALD. So this article that is dated May of this year really does not speak to your testimony and especially that that I have dated April, 2003?

Mr. WILLIAMS. That is correct. There is a learning curve on anything. The first time we used the system, there were some problems in some of the precincts, but these are mostly training issues and so forth.

We haven't talked much about training, but if you asked me what is the one thing you can do to improve your elections, the answer is, train your poll workers. And I don't care what kind of voting system you have got. A well-trained poll worker can overcome a lot of problems in a voting system; and, conversely, a poorly trained poll worker can cause you a lot of problems, no matter what your voting system.

Ms. MILLENDER-MCDONALD. I think it was Dr. Shamos who said test, test, test, train, train, train, or one of you said that. Who would be the most reliable training source to train persons, especially in the minority communities? Because they really still do not believe that their vote counts and that there is a reliable system that really speaks to their having security in voting.

Mr. WILLIAMS. In Georgia, we have a Center For Election Systems at Kennesaw State University. We provide training to county election superintendents, all 159 of them; and we do not train poll workers directly, but we train the people who train the poll workers. That is a huge effort that is ongoing.

Ms. MILLENDER-MCDONALD. I would think it is because you are training the persons who train the poll workers which you are not sure the poll workers are being trained, given the trainers that you have training them. If that is not a convoluted type statement, what else is? It is frustrating to sit here and hear this and to know those folks who are out there in the heartland and in the other part of our country are really frustrated about this whole voting system.

Mr. WILLIAMS. We have got hard statistics to demonstrate that we have greatly reduced the number of spoiled ballots in the predominantly minority districts.

Ms. MILLENDER-MCDONALD. Is that right? I would like to get that, if you can give me a copy of that.

Mr. WILLIAMS. Be happy to.

Ms. MILLENDER-MCDONALD. Is there anyone on this panel outside Dr. Rubin who thinks that the ballot, the paper ballot, is the best way to go? Is there anyone else here who thinks that, over and above the DRE?

Mr. KOHNO. I agree with that, especially in terms of between now and November.

I think the thing that I was trying to make before—the statement I was trying to make before is, the systems we know—we know the system we analyzed had serious security problems. We know that the certification processes don't address these security problems. So I think the thing to do in the short term definitely is that we need to—yes, to answer your question I think I do.

But I think I also wanted to—you were talking a lot about testing. I think one important thing to address is whether testing—I am sorry—not testing, you are talking about adding procedures, training people for procedures. I think the important thing to address is whether your having poll workers trained for election day is going to be sufficient enough.

One analogy I kind of like to think about was that we know that the systems right now may have a lot of security vulnerabilities. You are trying to rely on people and procedures to help protect the systems. An analogy you might want to talk about is like a bank saying, I know our safe doesn't work or I don't have a safe, but I am going to assume that no one is going to steal money because I have a lot of people walking around and following the procedures I have outlined.

One thing to keep in mind, the people implementing the procedures may be the adversaries as well.

Another thing, I was recently at a meeting at the Kennedy School of Government on electronic voting. One of the election officials there made a very interesting point. Her observation was that when people—anytime anyone starts a new job, you kind of expect them to make mistakes on their first day. That is not an unreasonable assumption. But the concern is that, for elections, every election day may be the first and only day for the people that are volunteering or being paid to work the polls that day.

These are two things to keep in mind, I think.

Ms. MILLENDER-MCDONALD. Let me ask one more question here. With the AAPD, the American Association of People with Disabilities, which one of these systems will best address their needs or if any of these will? A paper ballot? Braille?

Mr. RUBIN. I think the needs of the disabled community definitely need to be addressed with voting, and what has happened is we have taken in the design of the machines that are being used today like the Diebold machines, we have taken that as the predominant property to address. And it has been addressed. I think that it is possible to build systems that address those needs equally well and also address security. That hasn't happened yet. Having

a machine that allows a blind person to vote but also allows some malicious person to change the entire outcome of the election is not anything that anyone desires, not even a blind person. I think that we cannot ignore security.

Mr. SHAMOS. I don't agree exactly with that characterization. It is not a choice of one or the other. The disabled rightly argue that if there is going to be voter verifiability then they ought to be able to participate in that also. There are means of offering voter verifiability without the requirement of having a piece of paper which they cannot read.

So I am not against voter verifiability in any way. I am against attempting to accomplish it with paper where that paper becomes the official ballot. If you want to print out a piece of paper to convince the voter that her choices were correctly heard by the machine, there is nothing wrong with that. I just don't want that piece of paper to become the official ballot, because we have 150 years of history in which people with no training or education at all have been able to successfully manipulate those things.

It is true that there is no centralized manipulation possible with paper. The manipulations are only local. Whereas there is centralized manipulation possible with software, but it is the very centralization that makes it easier to detect.

Again, safes are not safe. Many banks have had safes broken into. That doesn't mean that we have disbanded the banking system. It may mean that it is necessary to hire more security guards and install video cameras to watch the safes.

But I disagree with the concept that perfection is required and as soon as someone points to some vulnerability we must shut down the entire system. There are security flaws of all kinds in these DRE systems, some much worse than others. Some are really excellent. Because there are security flaws, that doesn't mean that the election will necessarily be tampered with. It doesn't even necessarily mean that the probability will be high that the election will be tampered with. It means we have 25 years of history of using DRE machines and no one has been able to demonstrate that any election ever was tampered with, despite the fact that there have been numerous problems of all kinds, not necessarily related to security. So it is not a choice of one or the other. Paper certainly doesn't help the disabled, though.

Ms. MILLENDER-MCDONALD. Mr. Chairman, thank you so much for such an interesting and absolutely—although very thorough by the experts here, still very convoluted type of concern that we have, especially when we are preparing for the largest election in this country.

I note my dear friend and colleague Congressman Holt is here. He had a statement to submit for the record. By unanimous consent, may we have that?

The CHAIRMAN. The Congressman can submit it for the record, without objection.

Ms. MILLENDER-MCDONALD. Thank you, Mr. Chairman.
[The statement of Mr. Holt follows:]

HA 189.000

News from
Representative Rush Holt
 12th District, New Jersey
<http://www.house.gov/rholt>



For Immediate Release
 July 7, 2004

Contact: Jim Kapsis
 202-225-5801
 202-413-5277 (cell)

STATEMENT

Rep. Rush Holt Delivers Statement to House Administration Committee at Hearing on Electronic Voting Security

The process of voting must be fair, accessible and verifiable. While I have always supported increases in fairness and accessibility in the voting system, today I am focused on the verifiability, that is the auditability, of the voting system. I believe the auditability of our electoral system has not been given due attention, and has unjustifiably been treated as mutually exclusive to accessibility. We must take pains to uphold all three principles.

Voting is the foundation of democracy, and votes are inherently valuable. Anything valuable, such as bank records, or property records, must be auditable. We wouldn't have it any other way. The same absolutely must be true of our votes.

The process of voting in a democracy was always intended to belong strictly to the voter, who makes his or her decision and casts the ballot, and the election official, who counts it. A system such as this is "publicly" auditable, as it should be in a democracy – with the voters alone verifying that their intentions are properly recorded and the election officials alone verifying the accuracy of the tally. If a voter casts a vote on an electronic voting machine, verifying nothing but what is for a transitory moment in time reflected on the screen, how can the record of that vote be meaningfully audited? Can any election official, computer scientist, or voting system vendor reconstruct what that voter intended? No. The voter votes in secret. Because of the secret ballot, only the voter can verify that his or her intention is recorded correctly. That is why a hard copy of each vote – verified by the voter him or herself – must be required of all voting systems.

Voting systems that include hard copy paper ballots have been found to be among the most accurate of any voting system. The 2001 Caltech MIT study, "*Voting, What is, What Could Be*" reported that over the twelve-year period surveyed (1988-2000) "[o]ptically scanned paper and hand-counted paper ballots have consistently shown the best average performance. Scanners have the lowest rate of uncounted, unmarked, and spoiled ballots in presidential races and in Senate and gubernatorial races . . . Hand-counted paper has shown similarly low residual vote rates." The statistics reported were as follows: in presidential races, the residual vote rate as a percentage of all ballots cast was 1.8% for paper ballots, 1.5% for optically scanned paper ballots, and 2.3% for touch screen (DRE) machines. In Senate and gubernatorial races, the rates were 3.3%, 3.5% and 5.9%, respectively.

Besides having a worse residual vote rate than optically scanned and hand-counted paper-ballots, touch screen machines in their current form are not meaningfully auditable. This is fundamental. Better machines, better programmers, better procedures will not remove this problem. The report continued “[i]n the 2000 presidential election, the state of Florida conducted an enormous audit of its voting machines It is extremely important to be able to conduct such an audit. . . . Paper ballots have the highest degree of auditability. . . . The votes cast on a broken machine can never be reclaimed Most new electronic machines produce an internal paper tape (like a cashiers tape) and an electronic recording of every voting session. . . . While this is an improvement over [older DRE] machines, it is not a direct recording of the voter’s intention. If the machine fails between the touch screen and the tape, the voter’s stated intentions are still lost. We feel that new voting standards must require a minimum level of auditability.”

The touchscreen machines currently in use, which produce no voter verified paper trail, may count as many as 50 million ballots this November. Is there a possibility that the votes cast on those machines will be manipulated? Is it possible that the manipulation will go undetected? Of course it is. Numerous news accounts in recent years have reported irregularities in the results produced on electronic voting machines. The cause of each of those irregularities will always remain a matter of some speculation. But the bottom line is, inspection, testing and certification – all of which had been conducted on all of the machines in question – did not prevent those incidents. The integrity of those votes counts has been lost forever.

It is critical that all votes be independently auditable, which is only possible with systems that incorporate a voter verified paper audit trail. In the absence of an independent audit mechanism, the vote count will no longer be publicly owned. The voters will no longer verify the accuracy of their own ballots. No one else can. Because the software of virtually all electronic voting systems is protected by trade secret agreements, the American public is left to simply trust that, at the end of the day, the machines have given them the right answer. That is simply not acceptable in a democracy.

###

The CHAIRMAN. Mr. Larson, the Ranking Member, has another question, but, on the point, I think this discussion needs to be—everybody knows there is politics in this building, but this discussion really needs to—that is the way it has gone today—to rise above the political. There was a maligning editorial, I think a disgusting editorial on this whole issue—I mentioned this 2 weeks ago—really maligning people, especially people that are out there fighting for persons that have some form of disabilities. So there is the political side of this, the emotional side of this, but I think this type of hearing is a better way to look at the issue.

But, also, within the civil rights community and within the community of people that have some form of disability, they have genuine concerns about the paper ballots. I do not think it is just so clear-cut that you are either the good people if you are for the paper ballot or bad people if you question the merits of a paper trail. I don't think it is a clear-cut issue. I think there is some science to look at here and also the evolution of our elections. But the one thing for sure is we don't want people disenfranchised. That is the most important thing to consider.

Six years ago, Georgia's system had a high undervote rate. Dr. Williams answered 4.8 percent was the ballot error rate. In 2002, after deployment of the new systems that they have in Georgia, it was 0.87 percent, a fivefold reduction in undervoting. There were 71,000 votes in 2000 that no one voted at the top of the ticket; and now, under their system, it has been drastically reduced—if you hear 4.8 percent, that doesn't sound big, but 71,000 in that election was a lot of people. So am I correct in understanding that the undervote rate is down to 0.87, is that correct?

Mr. WILLIAMS. That is correct. We are not willing to give that up for concerns that have never occurred, for pure conjectures, when we have never yet had the first hint of problems. We have been using computer-based systems in Georgia since 1964. DeKalb and Fulton County were the first jurisdictions in the United States to count ballots on computers. In that whole period we have not once had anybody attack the computer system.

Ms. MILLENDER-MCDONALD. Mr. Chairman, just as a follow-up to what you are saying, Dr. Williams, what I am interested in is seeing in the minority community the reduction of the problems that have occurred since you are using DRE. If there is a comparison on your report that you are going to submit to me, I would like to see that as well.

Mr. WILLIAMS. The figures he is quoting are State averages. In some of the communities, those undervote rates were much higher than that. They went up to much higher numbers in some communities. What he is quoting is the average.

Ms. MILLENDER-MCDONALD. Mr. Chairman, in the City of Carson where we have a DRE, those voters, seems to me, that that electronic voting is much more secure than the paper voting, given the Florida's issue. However, since the whole notion of paper trail has come about, now they are concerned as to whether or not there is reliability. I suppose no matter how you cut this there will always be the chances of voters being concerned about the whole notion of whether their vote has been counted.

Mr. SHAMOS. Much recent analysis has gone into looking at the security of electronic voting systems, and it should. I completely agree with the notion that we need as complete a list as we possibly can have of the vulnerabilities. We also need transparency in these systems.

I am not aware of any recent studies where people have looked again at paper ballots, looked at the physical handling procedures for paper ballots to try to develop a list of vulnerabilities there. This country over a long period of time discarded paper ballots to the point where they are used in less than 1 percent—to cast less than 1 percent of the vote in this country. We have gone over to various other systems to eliminate chicanery.

When the lever machine was introduced in 1892, its inventor said of it that its purpose was to protect the voter mechanically from “rascaldom,” an interesting new term. I had never heard that before. I think it is pretty clear what rascaldom is, however. And that is because of rampant—once every 12 days since 1852—rampant stories of all kinds of tampering with paper ballots. So I think somebody should do a new study looking at whether paper is more or less secure than the voting systems that we know have security vulnerabilities.

Ms. MILLENDER-MCDONALD. I think that would only be fair, given that we have arguments on both sides, that we should look both places for that type of reliability.

The CHAIRMAN. The gentleman from Connecticut.

Mr. LARSON. Thank you. I thank the chairman for the great latitude that we have had this morning in exploring these issues because it is so important.

I would note this past Friday, in fact, we marked the 40th anniversary of the signing of the Civil Rights Act of 1964; and the gravity of this, of course, comes home today. Many people fought and gave their lives for the right to vote and how serious this is. I think across this panel and across this Nation, people are very much concerned. I think that is heartening to see.

Again, I want to commend the chairman, Mr. Hoyer and others for HAVA, because I do think—although I disagree with Mr. Mica, I think that it is important to have a funded mandate. For so long the States have had to bear an unfunded Federal mandate in handling all of our Federal elections. This provides an opportunity for them to receive the appropriate kind of money.

I want to go back because I think, as I listened to the testimony and hear the arguments put forward, Dr. Shamos, you said that if we strive for perfection, we can't get there given there has been no system designed to date that will allow for that. So, within that context, we have to look and see what the risk is and what was the risk analysis and what we can arrive at in terms of the best system.

It seems we have two goals in front of us. One ongoing, to continue to strive towards perfection as we project out into the future and the other a more immediate goal in terms of the November election whose backdrop is the election of 2000 and the concerns that have been raised.

I would add and it seems at least—and I don't want to put words in anyone's mouth—that there was a general consensus that in the

short term testing, testing, testing, training, training, training, testing with the Rubin corollary of independent sources is a very logical remedy, though I think Dr. Kohno would prefer that there be a paper trail that would go along with that, or as Peter Finley Dunn would say, trust everyone but cut the cards. But it seems to me at least in the short run that those seem to be goals that we could accomplish as the debate still goes on between whether or not the idea of trust and verify, of the paper trail being the best possible alternative for us to go to, the most secure alternative to go is further explored. Is that a fair statement? And how would you respond to that?

Mr. KOHNO. I guess I will respond since I was singled out as maybe disagreeing, but I actually don't disagree. I think that I would prefer to go back to the voter-verifiable paper ballot if we can, but it sounds like there are various procedures and various things that might prevent that. In that case I agree. You want to do the best you can to raise the bar in an attack. If that means you have to do more testing and do more secure analyses and changing the procedures, if that is actually the best you can implement, then I say you should at least do that.

Mr. SHAMOS. And I think paper has some use. It certainly has use in commercial transactions. One of its uses is to point out errors. So my belief is that if a voting machine is making a record and it is making a simultaneous record that the voter can see and there is some discrepancy between the machine record and the one that the voter sees, that is the starting point for investigation.

Forensic experts come in, they tear the thing apart, and they find out what is wrong with it. They don't propose that it is the right thing to do, to take the piece of paper and make that the official ballot, any more than it is right to take the electronic record and make it the official ballot if there is something wrong with it unless we can have adequate handling.

Mr. RUBIN. I am very impressed with your ability to extract all the points of agreement and consensus and I agree with your summary of our positions.

Mr. LARSON. Thank you.

The CHAIRMAN. I want to thank all four witnesses. I think it was a very, very fascinating hearing and I want to thank you for coming to the Capitol.

We will move on to the second panel. I want to thank the second panel for waiting a period of time. We have Linda Lamone, Administrator of the Maryland State Board of Elections; and Kathy Rogers, Director of Elections Administration, Office of the Georgia Secretary of State; and Jill Lavine, Registrar, Sacramento County, California. I want to thank all three of you for coming.

STATEMENTS OF LINDA H. LAMONE, ADMINISTRATOR, MARYLAND STATE BOARD OF ELECTIONS; KATHY ROGERS, DIRECTOR OF ELECTIONS ADMINISTRATION, OFFICE OF THE GEORGIA SECRETARY OF STATE; AND JILL LAVINE, REGISTRAR, SACRAMENTO COUNTY, CALIFORNIA

The CHAIRMAN. If we could, Ms. Lamone.

STATEMENT OF LINDA H. LAMONE

Ms. LAMONE. Thank you very much, Mr. Chairman, and members of the committee. I am more than pleased to be here today.

A lot of the discussion on the previous panel focused on the voting equipment, and I want to emphasize to you all that voting is not only the voting system; that it has many other components, and they involve people and procedures and those other components are equally important to the whole process.

The other thing that has been stressed this morning is testing. I think I can safely say that both Georgia and the State of Maryland test this equipment beyond what anybody ever expected or what we thought we would have to do. We have at least four preelection testing procedures that the equipment must survive successfully before it can be used in an election. That does not include the ITA or independent testing laboratories that do the testing to meet the Federal standards.

We also, when we do the testing in Maryland having anything to do with the software, we always involve two other entities besides my staff, and that is a quality assurance firm and something called an independent validation and verification. These are firms that we contract separately. They all have security clearances and the other credentials necessary.

So we have very high competence in Maryland that when we test this equipment, we are testing it to the highest standards and highest quality possible. We also do other testing, that Dr. Williams mentioned, in Georgia; and that is to make sure there are no Trojan horses or other malicious code. And I would think that since the Diebold—which we both use—voting equipment code has been in the public domain for a year, if there was malicious code or otherwise in that system, it would have certainly been discovered by all the hot-shot ITA people or information technology people that claim to know all about elections all of a sudden.

In Maryland, we have also had our voting system analyzed by two independent securities firms. One was the first one, SAIC, and the second one was done by a company out in Columbia, Maryland. We have had both firms report to us the risk assessments, the mitigations that they thought we should take and Diebold should take, and both of them assured me in their written reports that the voting equipment counted, recorded, and tabulated the votes 100 percent accurately. And again, that gave us a great deal of satisfaction and confidence in our voting system.

In addition, the SAIC also thoroughly investigated the work that was produced by Professor Rubin, and they made four recommendations to us, all four of which have been implemented in Maryland. One was to have the ability to protect the—or create the passwords on the voter access cards; two, the same thing with the activation cards or the memory chips on the voting equipment; three, randomize the votes; four, use encryption for any modem of the unofficial votes on election night. All four of those recommendations were implemented in Maryland prior to the March 2004 primary.

I think another interesting thing is that the computer scientists have all these things—conjecture could happen. It is conjecture that someone is going to be able to go out there and mass-repro-

duce the voter access cards so they can have access to the voting units and manipulate the election. They also say they are going to be able to do the same thing with the memory cards. Yet again, the source code has been in the public domain for a year and no one has successfully done that. No one. And I would suggest to the committee that if it were possible to have done so, they would have come forward to let the world know, because they like to tell people how well they can do things like that.

We are doing an upgrade of the system now, and we will do another whole security analysis this summer. I have three full-time employees on my staff that are devoted to nothing but security issues. We have developed with, again, another independent outside security firm for an entire information security plan for the office, not only on the voting system but on every aspect of the process of conducting elections, including voting registration.

A lot of the issues this morning also talked about the paper trail. And I understand, Congressman Larson, I appreciate your characterization of the positions because I think they accurately reflect mine and everyone else in the Nation who has to deal with the issue and who cares very deeply about having a secure and safe election.

But let me just show you what a paper trail would look like for one voter from Baltimore County, Maryland in the March 2, Super Tuesday primary. This is 10 feet long, one voter; and it took us 4½ minutes to print it out. Granted, we had to shut down the election to print the thing out because the system isn't geared right now to printing a contemporaneous paper trail. But that is a lot of paper per voter. You look at the turnout in the November primary or November general election, probably 80 percent in Maryland, it is going to be a lot of paper we are going to have to have.

And let me ask you, how are your constituents going to react when the printer paper jams and they say, Mr. Technician, will you come over here and help me unjam this paper trail, because the machine won't let you cast your ballot until you print this paper. When that technician walks over, he or she is going to be looking at a live ballot on the voting equipment. And for those of you who have optical scan balloting in your jurisdiction in the past, you know how protective the voters are. They don't want the poll workers to see their ballots. We use privacy screens to try to protect them. On the DRE, before you cast your ballot, your review ballot screen is live. It shows how the voter has voted, and that is what the technician is going to look at.

And I think you need to know that the printer engineering community at IEEE is convinced that the printers that the voting vendors are now producing are not going to meet the standards we need to have to have a safe and reliable election. Mr. Rubin had an experience as an election judge in Maryland, and he said when they went to close the election they had a discrepancy between the number of votes on the DRE units and the number of votes that they had checked in. I suggest to the committee that the reason was human error. The machines were correct. The people handling the pieces of paper, the voting authority cards, the poll books, had made a mistake.

And that is exactly what we are trying to get away from with the electronic voting equipment, aside from all of the other attributes that you have discussed here already.

The other thing that really, really irritates me and my colleagues around the country is the irresponsibility of the way the press has handled this issue. They start with one problem, and all of a sudden it is attributable to the voting units. Let me give you an example. In Maryland, right down the street from my office, they delivered the wrong encoders. That is the device that puts the ballot on the voter access card. They delivered the wrong encoders to a single precinct. It was human error. They simply mixed them up. And when they went to program the cards and the voter put them in the voting unit, it wouldn't pull up a ballot because it was the wrong encoder for the wrong voting units. It worked as it was supposed to work. I had international press at that precinct reporting that as an equipment failure, and that got perpetrated over and over and over again, that that was a major problem in Maryland. It wasn't a major problem. We didn't have any major problems in Maryland with the voting equipment.

Everything that happened that went wrong was attributable to human error. And that is because now we are boosting our training and voter education. We are spending millions of dollars on security, on training, on voter education, and we still get nailed in the press.

You asked what we are doing to get the word out. We can't get our word printed. We put out all this good stuff that we are doing. When we sit down to educate a reporter and finally teach him or her everything we do, they go in and say, wow, I had no idea you did that stuff.

CBS news was in Maryland a week ago Monday, and when my staff finished explaining to them everything we go through, they were convinced. We will see if they will actually broadcast that, which will be on this Sunday morning on Sunday morning news.

The other thing that the New York University Brennan report came out with is a lot of issues about each State should have a security analysis done like we have done in Maryland. Let me suggest that I think that we would have a lot better economy of scale if NIST or someone like that did it on each voting unit and provided it to the States so we could use our management and other procedures to then implement it and control it.

I see my time is up. I thank the committee for the opportunity to appear today.

The CHAIRMAN. As they always say, they don't report when the planes land, you know.

[The statement of Ms. Lamone follows:]

MARYLAND

STATE BOARD OF ELECTIONS
P.O. BOX 6486, ANNAPOLIS, MARYLAND 21401-0486 PHONE (410) 269-2840

Linda H. Lamone, Esq.
*Administrator*Timothy G. Augustine
Deputy AdministratorRoss Goldstein
Terry Holliday
*Candidacy and Campaign Finance***TESTIMONY BEFORE THE U.S. HOUSE OF REPRESENTATIVES**
Committee on House Administration
July 7, 2004**Linda H. Lamone, State Administrator of Elections**

Maryland had its own "Florida" in 1994. With less than 6,000 votes deciding the gubernatorial contest, Maryland's election systems and processes were heavily scrutinized and many recommendations were made to improve the conduct of elections in the State. The result of these studies led to an increased centralization of election functions, mandatory uniformity in processes and procedures, and maximizing the use of technology in election administration. These reform efforts placed Maryland in the forefront of election reform and positioned the State well for the implementation of the Help America Vote Act in 2002.

As with every other aspect of our lives, technology is a tool to improve processes and increase efficiencies. The impact of technology in election administration has been revolutionary. Technology has enabled election officials to improve the integrity of voter registration lists to ensure that only eligible voters vote, improve access to the electoral process by using voting equipment that is secure, accurate, recountable, and accessible, and reduce the likelihood of administrative error by automating traditionally manual processes.

While the benefits of technology in election administration are significant, election officials acknowledge that the introduction of technology brings additional responsibilities and requirements. Security protocols, risk assessments, and well qualified security personnel are becoming the norm in election offices around the country. Maryland has already implemented many of the security recommendations issued during the last year, and both in-house and independent security experts are continuously enhancing security procedures to protect the voting system and reassure the public of the accuracy and security of the voting system.

After 2000, Maryland replaced its unreliable and error-prone voting systems with a uniform statewide DRE voting system. Voters across the State now vote on Election Day on a DRE voting system and enjoy the significant advantages of this voting system. DRE voting systems are easy to use, eliminate issues of voter intent and "overvotes," enable most voters with disabilities to vote a secret ballot for the first time, and are capable of handling multiple languages.

When analyzing any voting system, it is critical to understand that a voting system includes more than just the equipment that records and tabulates the votes. It also includes the people (election officials and election judges), election laws, and the procedures that surround and govern the election process. The analyses performed by computer scientists and security experts have strengthened the electoral process but it is important to recognize that many of these

FAX (410) 974-2019
MD Relay Service (800) 735-2258Toll Free Phone Number (800) 222-8683
<http://www.elections.state.md.us>151 West Street, Suite 200
Annapolis, Maryland 21401

individuals and organizations are not election experts. While the computer and security experts' contributions are important, many of the procedures and processes that protect elections have not been incorporated into these analyses. For example, Maryland has an independent verification and validation performed to confirm the system's functionality and accuracy after a software upgrade has been loaded. Also, many of the security recommendations fail to recognize the realities of polling places where election judges, challengers, watchers, and other voters observe the voting process.

Vigorous testing of a voting system is critical to identify any malfunction before Election Day. Before a voting unit can be used in Maryland, all components of the voting system are subjected to repeated testing and must meet various voting system standards. Any voting system must be examined by an approved independent testing authority and shown to meet the performance and test standards established by the Federal Election Commission. Before use in an election, election officials cast a predetermined number of votes on every voting unit and compare the actual outcome with the expected outcome. After the ballot has been certified and loaded on each voting unit, election officials perform another test, "logic and accuracy" testing. During this test, each voting unit is set for Election Day, and again, a predetermined number of votes is cast on each voting unit. Each voting unit is sealed with tamper tape restricting access to the memory card and remains sealed until Election Day.

Maryland's voting system has been analyzed more than any other voting system in the country. In addition to the testing described above, numerous academics and third parties have reviewed the voting system. Additionally, I had the source code reviewed by an independent verification and validation security firm in Maryland. While these analyses did identify areas where security enhancements could and have been made, **all** of the analyses found that the voting system accurately records and tabulates votes. There was no finding of malicious code, and with the source code in the public domain for over a year now, I would expect that someone would have reported malicious code if it existed.

In addition to the concerns about malicious code, there are concerns about tampering with the voting system. Although any electronic voting system is hypothetically "hackable," I am confident that the likelihood of this occurring is extraordinarily remote. In order for this to occur, there would have to be an election official collaborating and assisting with this illegal effort. Reports implying or alleging this are insulting to your dedicated and honest election officials.

To "hack" into a voting system, the individuals would have to have access, assistance, and significant knowledge of the voting system. These individuals would also be committing a felony. They would have to:

- Have knowledge of the programming language in which the software was written;
- Have knowledge of every location in the software where it checks on itself to verify that the numbers it is reporting are accurate;
- Have knowledge of the program language and version of the compiler controlled solely by the independent testing authority that converts the program from a human readable form to machine language;
- Gain physical access to the software loaded onto 16,000⁺ voting units and 50⁺ servers for a long enough period to replace it. (Physical access is required because neither the voting units nor the servers are ever connected to the Internet.);
- Make the software ignore the pre-election tests during which the computer's internal clock is set for election day and only initiate itself on election day;

- Have the software be able to actually change votes throughout the day and do so **undetected**;
- Make the software able to erase or conceal itself before any post-election test;
- Have enough time to – without detection – either erase the Read Only Memory chips installed in the units or have enough supplies of identical chips that have been reprogrammed to be inserted into the unit;
- Have access a second time to remove the “malignant” chips after the election and replace them with the real ones removed prior to the election;
- Have knowledge of the up to 600 different ballot styles in Maryland;
- Have access in many jurisdictions to make the necessary changes to impact a Congressional or statewide contest; and
- Involve a significant number of people to make all this happen undetected.

Much of the national debate on voting systems has centered on the voter verified paper trail. While this public policy debate is occurring in Congress and in state governments around the country, I believe that the policy makers must understand the impact that requiring a voter verified paper trail to remedy the perceived inadequacies of the DRE voting systems will have on voters and election administration.

Before addressing the impact of requiring a voter verified paper trail, it is important to note that Maryland’s DRE voting system already enables a voter to verify electronically his or her votes before casting a ballot. A voter views a screen that shows the voter each contest on the ballot and the candidate for whom the voter voted. If the voter did not vote for a particular contest, the contest is highlighted in red to notify the voter of his or her failure to vote for that contest.

First, many of the perceived threats to electronic voting systems are just that – perceived. Since the introduction of electronic voting systems in this country, there has not been one single case of election fraud due to tampering of a voting system’s hardware or software. There have, however, been numerous cases of election fraud surrounding paper ballots.

Second, I would caution against legislating a specific technology to address the public perception. Requiring a *paper* trail would limit the development and use of alternative technology that provides the same or better type of verification to the voter. Maryland is currently exploring this technology and hopes to conduct a pilot before the next election cycle.

Third, the reintroduction of paper significantly impacts the voter and the election process. The following highlights some of the ways that voters and the election process will be impacted by adding a voter verified paper trail:

- It makes voting more complicated and time-consuming by requiring extra steps by the voter;
- It has the potential of tying the voter to his or her vote and violating ballot secrecy by either examining the sequence of the printed ballots or requiring an election judge to clear paper jams;
- It impacts the ability of the blind and the visually impaired to cast a secret ballot;
- It will require the voting equipment to print ballots in more than one language as required by the federal Voting Rights Act;
- It creates a false sense of security with the voters because it does not guarantee that the same results will be recorded within the memory as are shown on the paper;

- It presumes that voters will use the voter verified paper trail. If the majority of voters do not verify (as studies have suggested), the added value of the paper trail is diminished.;
- Hand counting the paper ballots is time-consuming and more error-prone than machine counting;
- There are no federal standards against which to test the method;
- It incorporates the problems inherent in a paper recount: mutilated or hard-to-read ballots, loss or manipulation of ballots and the fact that no two recounts yield the same result;
- Since the method is largely untested, it is not clear to what extent it would improve security in practice;
- The use of printers would increase the cost of administering an election and the risk of mechanical failure of a voting machine (printers jam, run out of paper, and can be slow);
- It increases the problems in recruiting and training election judges because of the additional requirements and steps they must perform; and
- It involves the transportation and storage of paper ballots.

One of the arguments for a voter verified paper trail is the inability of an electronic voting system to conduct a meaningful recount. With an accurate voting system that eliminates issues of voter intent and does not rely on human tabulation, we would *expect* the voting system to report the same results. Variations in recounts on other voting systems are attributable to voter intent issues and manual tabulation errors by the election officials recounting and tabulating the votes.

Under Maryland law, a voting system must be capable of creating a paper record of all votes cast in the event of a recount. There are several ways to conduct a recount on Maryland's current voting system, one of which is printing all of the ballot images and conducting a manual recount.

In Maryland's 2002 gubernatorial election, there was a recount in a legislative subdistrict. Because the legislative subdistrict crossed jurisdictional lines, there were two different voting systems involved in the recount, an optical scan voting system and a DRE voting system. As expected, there were no issues of voter intent with the DRE voting system, and the results from the recount matched the originally reported election results. On the other hand, a manual recount of the ballots tabulated by the optical scan voting system changed seven votes. The results from the recount on the optical scan voting system did not match the original results because the voting system failed to accurately capture the intent of seven voters.

While the recent debate regarding electronic voting has strengthened the security of electronic voting systems, it is important that the elections community have the flexibility to implement solutions that address the voting system concerns. The Election Assistance Commission has just begun its work, and it would be premature to mandate a technology-specific solution before the Commission's various boards have completed their studies and issued their recommendations. In the meantime, however, I believe that election officials can and are taking the necessary steps to ensure that the election process is secure, accurate, and reliable.

LINDA H. LAMONE

Linda H. Lamone was appointed by the Governor to be the State Administrator of Elections on July 1, 1997.

Ms. Lamone received a Bachelor of Science with honors from the University of Maryland, College of Business, and a Juris Doctorate with high honors from the University of Maryland, School of Law. She was elected a member of the Order of the Coif.

After graduation from law school, she joined the Office of the Attorney General of Maryland as an Assistant Attorney General in the office of Counsel to the General Assembly. During her tenure with that office, she also served as Counsel to the State Administrative Board of Election Laws from 1983 to 1987, as Special Counsel to the Administrative, Executive and Legislative Review Committee of the Maryland General Assembly, and as Counsel to the Board of Review of the Maryland Department of Agriculture. In 1987 she became Special Counsel to the Lt. Governor of Maryland. In addition, she has been in the private practice of law and, just prior to her appointment to her current position, was the Assistant Attorney General for the Maryland Higher Education Commission.

Ms. Lamone is the Vice Chair of the Attorney Grievance Commission of Maryland and is the Chair of the Character Committee for the Fifth Appellate Circuit. She is a former President of the Women's Bar Association of Maryland, the Women's Law Center of Anne Arundel County, the Select Committee on Gender Equality, and the Ballet Theater of Maryland. Ms. Lamone is a graduate of Leadership Maryland, is a member of the Board of Directors of the Maryland Governmental Relations Association, and she currently serves on the Executive Board and as President-Elect for the National Association of State Election Directors.

As the Maryland State Election Administrator, Ms. Lamone, has played a leading role in the implementation of innovative technology in election administration. Since her appointment in July 1997, Ms. Lamone has overseen the development and implementation of a statewide voter registration system and a mandate for a uniform statewide voting system. Additionally, Ms. Lamone directed the development of a sophisticated candidate and electronic campaign finance management program and an election management system that creates and certifies each ballot layout for the State of Maryland. Working with county election officials, she also implemented a uniform and comprehensive approach to election administration.

Ms. Lamone has made numerous presentations on election-related topics.

The CHAIRMAN. Ms. Rogers.

STATEMENT OF KATHY ROGERS

Ms. ROGERS. Thank you very much. As you know, the 2002 general election was a milestone in Georgia history as we became the very first State in the Nation to implement a statewide uniform electronic system of voting. On that one day on November 2, 2002, many concerns and fears were laid to rest. The elderly did not have trouble voting on Election Day and voters were not afraid of the new technology. For the very first time, every voter was afforded an opportunity to vote on the same equipment, using the same interface as their neighbor in the next county.

That fact seems to be forgotten today. By upgrading our voting system platform, Georgia corrected a problem which was very close to being a disaster. And in the almost 2 years since that very first successful election, Georgia counties have conducted over 450 individual elections using the statewide uniform electronic voting system. Georgia voters have expressed their approval in not one but two independent studies which were conducted by the University of Georgia. These studies found that Georgians overwhelmingly prefer electronic voting to any other means. More than 70 percent of the respondents reported they were very confident that their vote was accurately counted, and some 97 percent reported that they experienced no difficulties whatsoever when using electronic voting. These numbers have already been thrown out, but I don't think it hurts to reiterate them again.

Six years ago on our antiquated voting platforms, the top of the ballot of the U.S. Senate race was a 4.8 percent undervote rate of total ballots cast. Of enormous concern to us was also our analysis of 90 minority precincts in which we showed an extremely high undervote rate that in some cases topped 10 percent in predominantly African Americans precincts. After 2002 and the deployment of our new system, the undervote rate in the top of the ticket ballot was reduced to a mere .87 percent. That is a fivefold reduction in undervoting.

The paper receipt debate has generated a great deal of inaccurate, false, and misleading information by those who are calling for its very hurried implementation. Conspiracy theories do abound. No system, as has been stated earlier, whether electronic, mechanical, or paper based, can be made 100 percent invulnerable to attack; but the facts are the current system of voting is more secure than any type of voting that has ever been used in the history of Georgia elections.

We in the State of Georgia did not sign a contract with our vendor and simply walk away from the process. Rather, we have provided oversight and direction to our counties through every step of implementation and we continue to do so to date.

Let us consider the practical realities of paper receipt for just a moment. We have discussed how would each receipt be collected, how does the voter view it. You saw the prototype from Maryland. Georgia has created one that is about 31 inches long. It brings into question how you would store the paper for some 4 million voters in the State of Georgia and the voiding and the spoiling of the ballots.

I heard mentioned earlier the possibility of a paper shredder. I am not sure we want paper shredders in our polling places on Election Day. There is also the question of what is the official record of the election? I have heard a lot of controversy about which would be the official. If it is the paper, what happens if so much as one piece of that paper were to become mangled or destroyed? Have you then called your entire election into question?

If even 1 percent of Georgia precincts were to experience problems implementing a paper trail on Election Day, that would translate to 30 polling places in the State of Georgia. I can assure you if that were to happen, it would no doubt be portrayed as a catastrophic failure by the public and by the press.

We also find it very remarkable that even as many activists are calling for this hurried implementation of paper receipts, these same critics express no concern whatsoever over the 30 million Americans who will be voting on a punch-card system this November. We can be certain that hundreds upon thousands of Americans will be disenfranchised by these punch-card voting systems which have been proven to be far more inaccurate than our current system of voting. And yet we hear no impassioned pleas from journalists or the activists that these systems must be decertified before November, and we have to ask the question, Why?

We agree, as do all election officials, that we must continue to embrace a concept of continuous improvement in election security and we recognize that much of the debate has been healthy. And some of it has surfaced significant shortcomings which needed to be addressed.

We in Georgia cannot overstate the value of having an independent, technically competent center like the Kennesaw Center for Election Assistance which is staffed with elections-oriented computer scientists who are equipped to audit and test voting systems. Every day we continue to review our security practices. And over the last 18 months, we have strengthened our procedures and our practices a great deal.

I applaud the interest of this distinguished committee in the important public policy issue, and we stand ready from Georgia to assist you in any way that we can. Thank you.

The CHAIRMAN. Thank you for your testimony.

[The statement of Ms. Rogers follows:]

**Testimony before the
House Administration Committee
By
Kathy Rogers, Director, Georgia Elections Division
and
Britain J. Williams, Ph.D., Professor Emeritus
Of Computer Science and Information Technology
Kennesaw State University**

July 7, 2004

Introduction

The 2002 General Election was a milestone in Georgia history, as we became the first state in the nation to successfully implement a statewide uniform system of electronic voting. Georgia's transition to new electronic voting equipment was the result of an in-depth analysis of the accuracy and accessibility of available voting systems, an extensive statewide voter education program and poll worker training, and an unprecedented partnership between state and county governments.

In the almost two years following that first election, Georgia counties have conducted hundreds of elections using electronic voting. Numerous success stories have emerged from nearly every corner of the state. Two themes quickly emerged: Georgia voters young and old embraced and expressed confidence in the new voting system, and our state's under-vote rate was dramatically reduced following the deployment of the electronic voting platform. Georgia voters have overwhelmingly indicated their approval of electronic voting in not one but two independent public opinion studies conducted by the University of Georgia's Carl Vinson Institute.

In recent years a small group of political activists captured the attention of the media with the conjecture that direct recording electronic (DRE) voting machines are inherently not secure. Furthermore, they contend that the only way that these systems can be made secure is by the addition of a Voter Verifiable Paper Ballot (VVPB). These activists' conjectures gained respectability when they were joined by several computer scientists from major universities. These academics claim that computer systems in general and voting systems in particular cannot be made secure.

A DRE voting system is a comparatively simple computer application. The main line of the system is to respond to a touch at a specific location on a touch-sensitive screen and add one to the appropriate register. There is no requirement for intricate or complex computations. There is no requirement to compute any logarithmic functions, trigonometric functions, or even take the square root of anything.

The conjecture that using current technology we are unable to make such a simple system secure and accurate is contradicted by the facts of our daily existence. We build secure

and accurate computer systems that fly our airliners. We build secure and accurate computer systems that guide our submarines under the ice cap. We build secure and accurate computer systems that guide our astronauts to the moon and bring them safely back to earth. We submit to open heart surgery while a computer monitors our vital signs and controls an artificial heart and lung machine. The list of secure and accurate computer systems that monitor, control, and improve our lives is large and growing daily.

This is not to imply that our current DRE voting systems do not need to be improved. They do. But there are many aspects to a voting system other than accuracy and security. These include availability, reliability, maintainability, usability, and even affordability. Any change to a voting system must be evaluated on the basis of its impact upon the entire system. To this end Congress has created the Election Assistance Commission (EAC). This Commission has the resources and authority required to affect an orderly and disciplined evaluation of the state of the existing voting system technology and implement improvements to voting systems in an orderly manner.

The evidence is compelling that a rapid, poorly formulated forced addition of a paper ballot or receipt to the existing DRE voting systems is unnecessary and could have adverse consequences that far offset any perceived advantages. There is, in fact, no credible evidence that we are in imminent danger of a corrupted elections process created by new DRE voting systems. There is sufficient time, and a clear rationale, to allow the organizations and processes defined in the Help America Vote Act to perform their assigned duties and responsibilities.

To understand our perspective in Georgia and why we so strongly advocate the advantages of current generation electronic voting technology, it is important to know where we've been and why we took the path towards a uniform statewide DRE system.

Georgia's 2000 Election Experience

The 2000 Presidential Election served as a huge wake up call to a nation of voters and election officials. Alarmed by the high percentage of under-votes recorded by voting equipment in Florida, Georgia Secretary of State Cathy Cox compiled data on under-votes that occurred with Georgia's then existing voting equipment; a mix of lever, punch-card, optical scan and even paper ballots. The findings of that study were staggering. Not only did Georgia have a higher under-vote rate than Florida; at 3.5% our under-vote rate far exceeded the national average of 1.9% and was reported by the CalTech/MIT study as the third-highest in America. A study entitled "A Wake-Up Call for Election Reform and Change" was subsequently produced by the Secretary of State outlining the performance of Georgia's election equipment in each of its 159 counties during the 2000 General Election. Further analysis documented extremely large variations in under-vote rates between counties, as well as large under-vote variations between majority vs. minority precincts in the same county using the same equipment. In 2001 the ACLU, on behalf of several Georgia voters, sued the state, noting that, based upon the state's own data; the election platform then in place had a discriminatory impact and served to disenfranchise minority voters in counties throughout the state.

The findings in the “Wake Up Call” report were alarming enough that in 2001 the Georgia General Assembly passed, at the request of the Secretary of State, Senate Bill 213 which provided for the creation of a 21st Century Voting Commission. This group was tasked with studying the accuracy and reliability of all nationally qualified voting systems and to provide a report on its findings and recommendations to the General Assembly. This Commission was comprised of a balanced, multi-partisan group of General Assembly members, election officials, technology experts, and other important stakeholders. The commission invested a significant amount of time studying reports on existing technology, visiting other states to observe elections using electronic voting systems, holding meetings to obtain public comment, and, most importantly, overseeing an electronic voting pilot project.

In November 2001, 13 cities participated in a pilot project, utilizing six different NASED-qualified and state-certified DRE systems from six different vendors, to conduct actual municipal elections. The cities were selected to assure geographic, demographic and partisan diversity. The University of Georgia’s Survey Research Center was retained to perform an intercept, or “exit poll,” of voters to measure their reactions to the equipment and attitudes about the deployment of new voting technologies.

Altogether, the State conducted a full year of study, evaluation and due diligence before making its recommendation for voting system reform. In January 2002 the 21st Century Voting Commission unanimously recommended to the Governor and General Assembly that Georgia adopt a statewide uniform system employing electronic voting equipment.

Election Day 2002

November 2, 2002 was an historic day for Georgia. For the first time, every voter was afforded the opportunity to cast a ballot in the same manner using the same equipment with precisely the same voting interface. A voter in one county did not receive the advantage of better technology while his counterpart in a neighboring county voted on antiquated voting equipment prone to high error rates. That fact sometimes seems to be forgotten today. By upgrading its voting platform Georgia corrected a problem that was close to being a disaster.

In that single day many concerns and fears were laid to rest; the elderly did not have difficulty voting and voters were not afraid of the new technology. Blind and visually-impaired voters who had previously never cast a ballot independently expressed their feeling of pride and accomplishment at being able to utilize the features of electronic voting that allowed them to vote unassisted for the first time.

Electronic voting has removed the opportunity for fraud and error that inevitably comes when humans record votes on paper and handle and count paper ballots. In light of the current clamor for the addition of a paper receipt, it is worth noting that every single documented case of election fraud in recent Georgia history has involved the use of a paper ballot.

Georgia has taken huge strides in improving accuracy and ease of use, and the data gives us reason to be confident that a much higher percentage of the ballots cast in Georgia in November 2002 represented a true and accurate reflection of the voter's intent. Voters are allowed to review their ballot prior to touching the cast ballot button. No system has ever provided that capability before.

Six years ago, under Georgia's antiquated voting platform, the top-of-the ballot U.S. Senate under-vote was 4.8% of ballots cast. In 2002, after deployment of the new electronic system, the under-vote in the top-of-the ballot U.S. Senate race (an "apples to apples" comparison of system performance) was a mere 0.87 percent. That is a more than five-fold reduction in under-voting, a decrease of 71,000 ballots that showed no choice in the top of the ticket race. This is clear and convincing evidence that an electronic voting platform that prohibits over-votes, that provides the voter with feedback and that offers a summary screen to check and review ballot choices can dramatically improve the accuracy of the vote count.

Voter Confidence Validated

The Carl Vinson Institute of Government at the University of Georgia conducted a public opinion survey following the 2002 General Election and found that Georgians overwhelmingly prefer electronic voting to other methods. More than 70% of respondents reported being "very confident" that their vote was accurately counted, a sharp increase from the 56% who responded to that same question during the 2001 pilot project. Some 97% of voters said they "experienced no difficulties" when using electronic voting terminals.

The Vinson Institute followed up with a second survey one year later, in November 2003, which confirmed that over 70% of voters are still confident in Georgia's electronic voting platform. This same survey also noted that all voters in all age groups, income and education levels, and racial and ethnic groupings believe that electronic voting is superior to forms of voting previously used in Georgia.

The Arguments For, and Against, Voter Verifiable Paper Ballots

Those who distrust current DRE voting systems and believe they are easily manipulated to create fraudulent election outcomes have prescribed what they claim is foolproof solution: the addition of a paper receipt, or voter verifiable paper ballot. These claims warrant close examination.

When we vote to elect the members of the board of directors of a company, to elect the officers of a social or civic club, or to elect the officers of a labor union we cast a "ballot" (sometimes called a proxy). This ballot contains unique identifiers such as a signature, social security number, or member number that can be used by the election monitors to

validate the ballots. Given the ease with which the individual ballots can be validated it is unusual for the persons conducting these types of elections to expend the effort and expense necessary to purchase and implement a commercial, NASED Qualified voting system. They typically gather the votes and use their in-house computer technicians to develop a system to tally the votes. Any anomaly or challenge can be resolved by resorting to the verified ballots.

When we vote in a municipal, state, or federal election we do not cast a ballot in the manner described above. We cast a “secret” ballot, and this is an essential distinction. This ballot, by law, can contain no unique identifier that will enable anyone, including the voter, to identify the person who cast the ballot. Thus, in a municipal, state, or federal election there cannot exist a truly “Voter Verifiable Ballot”, paper or otherwise

The only paper output that can be added to a DRE voting system is the capability to produce a paper “receipt”. There are at least three DRE voting systems in the process of obtaining NASED Qualification that have the ability to produce a paper receipt. These systems demonstrate the problems that can result from attempts to implement modifications to a voting system in the absence of clearly defined, well thought out standards.

The EAC Voting System Standards (formerly known as the FEC Voting System Standards) do not currently contain a specification for a paper receipt produced by a DRE voting machine. The voting systems that produce paper receipts are being NASED Qualified under a provision of the Standards that permits optional features. In particular, the Standards require that a voting system comply with its own documentation. If the voting system documentation defines an optional feature (i.e. a printed receipt) then the Independent Test Agency (ITA) verifies that this feature is implemented in the system exactly as defined in the documentation.

As a result, the paper receipts produced by the voting systems currently seeking NASED qualification do not comply with the EAC Standards requirements for a ballot. For example, these systems will not comply with the Standards requirement for high contrast or increased print size to accommodate a person with impaired vision. Also, they will not comply with the Standards requirement to produce ballots in multiple languages.

Operational Considerations of Adding Paper Receipt

Experience has taught us that the deployment of a significant new addition to a DRE platform must also be examined in the light of Election Day reality. The success or failure of any voting system rests on the shoulders of poll managers and poll workers, who are, after all, citizen volunteers, many of them elderly, paid a very modest sum to operate voting equipment perhaps only once or twice a year. Paper receipt advocates who compare them to employees at WalMart or Target miss the mark entirely - poll workers are not and never will be full-fledged employees, who can expect regular sessions of training and who have multiple levels of professional supervision at their workplace. Therefore, not only must poll workers be carefully trained, but equipment

must be designed to minimize the technical and operational requirements they need to master in order to carry out a successful election. If, because of the demands of new and more complicated equipment that includes printers and related components, even one percent of Georgia precincts experience problems making their polling places operational on election morning, that translates into more than 30 precincts unable to allow voting to take place; a situation that no doubt would be portrayed by the media and perceived by the public as a catastrophic failure.

Just as important, we should make absolutely certain that the addition of a paper receipt function, if implemented, does not put us back into unacceptably high under-vote rates that we have worked so hard to overcome. In the sterile environment of a computer science laboratory, a new paper receipt prototype may appear simple and fool proof. But in the real world of elections, with equipment that must be accessible to voters with widely divergent levels of education, literacy, language proficiency, experience and physical ability or disability, it is crucial that the user interface be simple, straightforward and intuitive. Georgia spent enormous time studying this very issue, and the experience of other jurisdictions, before adopting a modern DRE platform as its preferred model. That due diligence paid off with plummeting under-vote rates - across all demographic groupings - and a much more accurate election outcome that re-enfranchised tens of thousands of voters. It would be tragic if a hurried, and inadequately researched, requirement for a paper receipt function makes the voter interface so complicated that it increases voter confusion and drives back upward the incidence of under-voting.

We Are Not in Imminent Danger

Computers have been used to tally elections in America since October, 1964 when DeKalb County and Fulton County, Georgia were the first jurisdictions in America to employ a punch-card voting system. Since then the State has used every type of computer-based voting system: punch-card, central count optical scan, precinct based optical scan, and direct recording electronic voting systems. During these forty years there have been many attempts to defraud a Georgia election, but not a single one of these attempts has involved an attack on the computer system. This is probably due, at least in part, to the fact that many people believe that they know how to successfully alter a piece of paper, but very few people believe that they have the ability required to successfully alter a computer system.

The Georgia DRE voting system is both accurate and secure. Measures are in place to insure that the voting system computers are as accurate and secure as current computer technology permits. In addition, physical security measures, an essential ingredient to secure elections and a topic that is often ignored by the critics of DRE systems, are in place to compensate for the remaining vulnerabilities that have been identified in the computer system. An extensive, statewide training program has been implemented to prepare our election officials and poll workers to recognize and react to any problems that may occur during the course of an election.

The Role of the KSU Center for Election Systems in Georgia

The Center for Election Systems at Kennesaw State University was created in 2002 to provide support and independent testing to all 159 Georgia counties. The Center for Election Systems at KSU tested every touch screen unit, encoder, optical scan ballot reader and server used in the 2002 General election. Tens of thousands of voting terminals and related components were tested by the Center, and its staff continues to travel to each of Georgia's 159 counties to independently test and validate all new equipment purchases.

In addition to testing, The Center for Election Systems now offers support to counties and their staff in the areas of poll worker training, enhanced courses on election management training, and courses for new election officials.

Election System Security Has Multiple Components

Those who are charged with conducting elections understand that the security of an election does not rest on the performance of equipment alone - whatever that voting platform may be. These election experts are well acquainted with the entire umbrella of security that surrounds the voting process. Every feature of the comprehensive security protocol, including paperwork procedures and physical security, is important to assuring the integrity of the voting process. A secure and accurate election begins long before Election Day and is comprised of many levels and layers of testing.

Computer System Security in the Georgia Voting System

Georgia has been a full participant in the EAC Voting Systems Standards project since its inception. Before a voting system can be considered for use in Georgia, it must be examined by the ITAs for compliance with the EAC Voting System Standards. Georgia considers a voting system to consist of a specific version of each of the system components: hardware, voting system software, and operating system software. Any change to any component, no matter how insignificant, is considered a different system and requires re-examination, both NASED Qualification and State Certification, of the entire system.

When a voting system successfully completes ITA qualification testing and is issued a NASED qualification number, it can be brought into Georgia for State Certification Testing. The system to be tested is not obtained from the vendor but is transmitted to the KSU Center for Election Systems directly from the ITAs.

The KSU Center for Election Systems conducts a series of tests on the system. Some tests examine the level of difficulty associated with operating the system. Another tests the capacity of the system to accommodate the maximum number of ballots that might be cast in a large precinct or at an in-person absentee voting location. One test is specifically designed by the KSU Center for Information Security, Education, and Awareness to detect fraudulent or malicious code that might be present in the system. This test is designed to wake up any, so called, Trojan horse that might be present. In all

of these tests a known pattern of votes is cast and compared with the output of the system.

If any of these tests result in a modification to the system, the entire system is returned to the vendor for correction and the NASED Qualification/ State Certification test cycle is repeated.

When the system successfully passes State Certification and is certified for use in Georgia, the KSU Center for Election Systems prepares an electronic signature of the system and archives the software source code and object code. The vendor is then authorized to install the system in the 159 county election offices. The primary reason for allowing the vendor to perform the installation is to protect the warranty on the system.

When the vendor notifies the State that they have completed installation in a particular county, the KSU Center for Election Systems sends a team to the county to conduct Acceptance Tests. These tests verify that the hardware is operating correctly and that the correct version of the software has been installed. During these tests the electronic signature of the software installed in the county is compared with the electronic signature of the software archived by the KSU Center for Election Systems to validate that the county system is identical to the system that was State certified.

The following describes three distinct objectives that are attained in order to insure the security and integrity of the Georgia voting system.

Objective 1: Verify that the voting system, as delivered from the ITAs, is free from extraneous or fraudulent code.

To attain this objective the KSU Center for Election Systems performs the following activities:

- Setup and conduct sample elections with known outcomes that are representative of Georgia general and primary election.
- Conduct high-volume tests to determine capacity limits of the system.
- Conduct tests to determine the systems ability to recover from various types of errors.
- Conduct tests to detect extraneous or fraudulent code.

Objective 2: Verify that the system as installed by the vendor in the local jurisdictions is identical to the system received from the ITAs and certified by the KSU Center for Election Systems.

To attain this objective the KSU Center for Election Systems performs the following activities:

- Prepare a validation program that will detect any changes to the system installed in the local jurisdictions.

- Run the validation program against the system installed in the local jurisdiction (after vendor installation).
- Provide the local jurisdiction with the ability to run the validation program.

Objective 3: Verify at specific and random times that the system has not been modified in any way.

Local Election Superintendents have the ability perform the following activities:

- Run the validation program immediately before beginning to define an election.
- Run the validation program immediately upon the completion of an election.
- Run the validation program after any suspicious event. Run the validation program at random times.

The validation program that is used to validate the correctness of installed systems is based on NIST certified SHA-1 contained in FIPS 180-2, August 2002 and includes the following:

32 bit CRC
128 bit MD 5 Hash
160 bit SHA-1 Hash

It is estimated that the chance of modifying the software in such a manner that this hash would not detect the modification is less than 1 in 1,000,000,000.

Procedural Security in the Georgia Voting System

Rigid policies and procedures are in place that control who can access to the election system, when they can access the system, what components they can access, and what function they are allowed to perform. The most familiar of these procedures is the process that a voter must go through in order to cast a vote on the system. Other procedures define the activities of election officials and poll workers.

Many of these procedures are directed toward insuring that the correct versions of the system software is initially installed in the election management system computers and voting stations and, subsequently, testing at various times to insure that this software has not been altered. We have already discussed this process.

Accuracy and uniformity of the ballots is critical to the success of an election. If a county so desires, the KSU Center will prepare the county ballot. Before the 2004 Presidential Primary Election the KSU Center prepared the ballots for 102 of the State's 159 counties. To achieve ballot accuracy and uniformity, the KSU Center for Election Systems reviews the ballot formats from all counties prior to each election.

Physical Security in the Georgia Voting System

The first line of security defense in any system is physical security. All other security measures go for naught if you leave the doors unlocked. The following is an overview of the physical security implemented in the Georgia voting system.

The election management system computers are kept in locked offices within the county election offices.

The election management system computers are not connected to any communication system, including the Internet, and contain no software other than the Windows operating system and its utilities and the election management system object code.

No person is allowed access to the election management system computer until his or her identity and purpose have been clearly established by the county Election Superintendent.

The voting stations are stored in their voting booth cases in locked county warehouse facilities.

At the precincts the PC memory cards in the touch screen voting stations are in a locked compartment on the voting stations. The Precinct Manager is the only person in a precinct with a key to this compartment.

After the polls close a printed report of the precinct results is posted on the precinct door. This places the results from the precinct in the public domain and any subsequent alteration of these results is easily detected.

The PC memory cards from a precinct are transported from the precinct to the county elections office by a sworn election official or a sworn law enforcement officer. Precinct managers may, at their option, send the precinct results to the county office via modem. However, these modem results are unofficial and are for the benefit of the press and the candidates. The official results are always computed directly from the memory cards.

The area of the precinct that contains the voting stations is secure. A voter is not allowed to enter this area until a voting station is available for his or her use. However, there are no enclosed voting booths and the secure area is in plain view of the poll workers, candidate representatives, party poll watchers, advocacy poll watchers, and media representatives. Any unusual behavior by a voter will be immediately detected.

Training and Ballot Building for Georgia Elections

One benefit of using a uniform technology throughout the State is that many ballot building procedures can be centralized. This enables better error detection and correction

as well as efficiency in the production of redundant ballot content (federal and statewide races and issues). Ballots can be reviewed for compliance with State law as well as proper district and precinct information. In the most recent statewide election the KSU Center for Election Systems prepared the ballots for 102 of the States' 159 counties. The KSU Center reviews all ballots, regardless of who prepared them, for accuracy and completeness. Following this review the ballots are returned to the counties for final review and acceptance.

The training issues in election technologies are unique. The process is heavily dependent upon personnel that are both volunteer and infrequent users of the system. The processes are a combination of manual and computerized operations that are the result of state and federal election law, state election rules, election tradition, and functional requirements of the election technologies. The processes are dynamic and change in varying degrees from election to election, requiring a constant vigilance of training objectives, materials, and curriculum. The KSU Center is responsible for working with the vendor and state and county officials in the development and maintenance of training programs.

In 2003 the State of Georgia enacted legislation that requires all election superintendents to successfully complete 64 hours of training. This training program includes election law, ethics, and election procedures, including those unique to the current DRE technology use in Georgia. This training helps to insure that appropriate security procedures are understood and implemented at the county and precinct level.

Conclusion

Members of this Committee as well as all election officials and policymakers have a difficult task - to sift through the rhetoric and headlines and accusations, some of them the product of partisan resentments - to separate fact from fiction and carefully assess the strengths and vulnerabilities of voting system alternatives. The claims and assertions of electronic voting opponents must be scrutinized with the same ferocity that has been applied to the statements and actions of equipment vendors and election officials. The successful experience of Georgia, and our enormous increase in accuracy and accessibility with minimal operational flaws and zero -not one - documented case of vote tampering or fraud - should be weighed as well.

No one knowledgeable about elections would come before you and claim that the current system are the best that can ever be devised, or suggest to you that we cannot make even more accurate, accessible and secure the systems that are now in use. A culture of continuous improvement is one that we have adopted in Georgia elections, and one that should be embraced by every jurisdiction. And so we applaud all those who offer responsible, well-reasoned criticisms and who have carefully considered recommendations for improvement. I am confident that this Committee will exercise great care and discernment in evaluating electronic voting systems, as we all strive to improve still further America's system of elections and voting.

Thank you for the opportunity to share my thoughts with this distinguished panel.

About the Authors:

Kathy Rogers is the Director of Elections Administration for the Georgia Office of Secretary of State. Ms. Rogers joined the Secretary of State's office in 2002 to spearhead implementation of the uniform touch-screen voting system adopted by the State of Georgia. Prior to joining the Secretary of State's team, Ms. Rogers served as the Election Supervisor for Chatham County Board of Elections (Savannah, Georgia). Ms. Rogers has almost two decades of election experience and has conducted elections with various types of voting equipment during her career. Ms. Rogers participates in several election organizations including the Georgia Election Officials Association, the National Election Organization known as IACREOT, the National Association of State Election Directors, the national Election Center, and also represents the State of Georgia on the newly created Help America Vote Advisory Board. Ms. Rogers recently graduated as a Certified Elections and Registration Administrator through a program administered by the Election Center and Auburn University.

Brit Williams is Professor Emeritus of Computer Science and Information Systems at Kennesaw State University. He was a consultant to the FEC during the development of the FEC Voting System Standards in 1990 and again in 2002. He is currently a member of the NASED Voting Systems Board and Chair of the NASED Voting Systems Board Technical Committee. He represents NASED on the newly created Help America Vote Technical Guidelines Development Committee. Dr. Williams has been conducting certification evaluations of computer-based voting systems for the State of Georgia since 1986. He also assists the states of Pennsylvania, Maryland and Virginia with certification evaluations of computer-based voting systems.

Kathy Rogers is the Director of Elections Administration for the Georgia Office of Secretary of State. Ms. Rogers joined the Secretary of State's office in 2002 to spearhead implementation of the uniform touch-screen voting system adopted by the State of Georgia. Prior to joining the Secretary of State's team, Ms. Rogers served as the Election Supervisor for Chatham County Board of Elections (Savannah, Georgia). Ms. Rogers has almost two decades of election experience and has conducted elections with various types of voting equipment during her career. Ms. Rogers participates in several election organizations including the Georgia Election Officials Association, the National Election Organization known as IACREOT, the National Association of State Election Directors, the national Election Center, and also represents the State of Georgia on the newly created Help America Vote Advisory Board. Ms. Rogers recently graduated as a Certified Elections and Registration Administrator through a program administered by the Election Center and Auburn University.

The CHAIRMAN. And we will move on to the last witness.

STATEMENT OF JILL LAVINE, REGISTRAR, SACRAMENTO COUNTY, CALIFORNIA

Ms. LAVINE. Thank you. I am Jill Lavine and I am from Sacramento, California. And Sacramento County was the first jurisdiction in the United States that has conducted any portion of an election using touch-screen technology that was incorporated in a voter-verified paper audit trail. Ours was a very limited early voting project which is described in detail in my written report. The equipment for this pilot was the Vote Trakker system provided to Sacramento County by Avante International Technology, Incorporated. The pilot was authorized by the Voting Systems and Standards Procedure panel within the Office of the California Secretary of State. Additional authorization was provided by the Sacramento County Board of Supervisors.

This project involved early voting in six locations for a period of 11 days prior to the November 5, 2002 election. Voters from anywhere in Sacramento County were permitted to vote at any one of the six locations. There were a total of 246 variations of the ballot for this election. The voting units were accessible for blind voters, to voters with disabilities, and each voter was able to choose a language: Spanish or English. A total of 1,612 valid ballots were cast at these early voting locations.

This experiment with the voter-verified paper audit trail was conducted under very controlled conditions. Each of the early voting sites was staffed with various personnel from our office and a technician provided by Avante. The equipment and the system met our requirements and expectations. We considered the project a success. The reaction to the equipment was mostly positive. Comments and observations from the poll workers, voters in the poll, and the others are contained in my written report.

In the interest of time, I will limit my time to the use of the printed ballot and the challenges it presented. Some of the voters did not want to see the ballot and fled before the ballot was able to print. There are approximately 20 of these voters. This could be a major problem. If a voter walks away before approving the paper version of the ballot, is the ballot counted? Some voters wanted to take the copy with them. We called the printed copy a receipt, which implied they could take it with them. This is obviously a mistake and is easy to change. The printed ballot jammed. This caused the machine to be taken out of service until the problem was corrected. In order to remove the jammed ballots, we had to use anything that was handy. For example, a back-scratcher and a windshield wiper blade were used to pull the ballots out. Voters complained that the printed copy of the ballot was hard to read because of the size and lightness of the print and because of the location of the shield which protected the printed copy. These problems are easy to correct.

Voters also complained that the length of the ballot made it difficult to check, which will continue to be a problem when the ballot is long.

Voters wanted to remove the printed ballot before it went back in the machine. This is not possible, of course, because a voter

could remove the ballot without being detected. Some of the voters were concerned that other voters would see his or her ballot. This was a placement problem that can be corrected. The location of the shield that protected the printed ballot made it difficult for a seated voter to see his or her ballot. Again, this is fairly easy to correct. The storage area for the printed ballot was too small and needed to be emptied during the day. This is obviously unacceptable and must be corrected.

After the voter verified his or her ballot on the screen, the printed version was produced. If the voter changed his or her mind, or didn't agree with what was printed, it was too late to be corrected. This has been corrected, but it is still potentially problematic.

Only ballots approved by the voters should be counted. At the same time, there must be no way to connect the ballot with a voter. During the canvass of the vote, we manually recounted one of the early voting places. The precinct selected had 114 ballots. Because of the complexity of the ballot and the fact there were 246 different ballot types, it took 127½ hours to recount. The machine count and the count on the paper ballots did match. Following this demonstration project, Avante made numerous changes to the equipment, addressing most if not all of the concerns expressed.

In conclusion, while a voter-verified paper trail may increase a voter's confidence in the use of electronic ballots, it is not without concern. While many of the concerns I have identified can and have been resolved, there still remain concerns that may not be fixable. For example at the polling place, the problem with fleeing voters, printing jams, the length of time necessary for a voter to verify his or her ballot. After the election, there would be significant delays in providing official election results from the manual counting of paper ballots in case of a recount or a challenged election. These issues remain unresolved.

Thank you.

The CHAIRMAN. Thank you for your testimony.

[The statement of Ms. Lavine follows:]

**HOUSE ADMINISTRATION COMMITTEE HEARING ON
BALLOT SECURITY, JULY 7, 2004**

**TESTIMONY OF JILL LAVINE, REGISTRAR OF VOTERS
COUNTY OF SACRAMENTO CALIFORNIA**

Chairman Ney, Committee Members

Thank you for this opportunity to address your Committee on the subject of ballot security.

I am Jill LaVine, the Registrar of Voters for the County of Sacramento, California. I am responsible for registering voters, maintaining the voter file, local campaign filings and the conduct of Federal, State, County and City elections within Sacramento County. In addition, I conduct the elections for more than 100 school and special districts. We have about 600,000 registered voters. I have been involved in the administration of elections in different capacities for more than 20 years.

Sacramento County, I believe, is the only jurisdiction in the United States that has conducted any portion of an election using touch screen technology that incorporated a voter verified paper audit trail. Ours was a very limited early voting pilot project which is described in a detailed report that I have provided. The equipment for this pilot, the Vote Trakker system, was provided to Sacramento County by Avante International Technology, Incorporated, without cost. The pilot was authorized by the Voting Systems and Procedure Panel within the Office of the California Secretary of State. Additional authorization was provided by the Sacramento County Board of Supervisors. I will briefly summarize our experience.

The project involved early voting in six locations for a period of eleven days prior to the November 5, 2002 Election. Voters from anywhere in Sacramento County were permitted to vote at any one of the six locations. There were a total of 246 variations of the ballot for this election. The voting units were accessible to blind voters (*nine used the voice-assisted provision*) and to voters with disabilities (*several were in wheelchairs*). Each voter was able to choose to have his or her ballot presented in either English or Spanish (*10 voters used the Spanish alternative language for casting his or her vote*). A total of 1,612 valid ballots were cast at the early voting locations.

A voter would come into the polling place, fill out a request for a ballot. The Voter's request would then be verified by a precinct worker using a laptop computer that accessed the County's voter file. A smart card was then programmed for their ballot type and given to the voter to insert in one of the voting machines. The voter would then make their choices on the screen, and then after selecting the cast ballot button the paper receipt would print. The voter then reviewed the receipt before it was pulled back into the machine.

This experiment with a voter verified paper audit trail was conducted under very controlled conditions. Each of the early voting sites was staffed with experienced personnel including a technician provided by Avante. The equipment and system met our requirements and expectations. We considered the project a success.

The reaction to the equipment was mostly positive. Comments and observations from poll workers and voters are contained in my written report.

In the interest of time, I will limit my comments to the use of the printed ballot and the challenges that it presented.

- Some voters did not want to see the ballot and fled before waiting for the ballot to print. There were approximately 20 of these voters. This could be a major problem. If a voter walks away before approving the paper version of the ballot, is the ballot counted?
- Some voters wanted to take the copy with them. We called the printed copy a "receipt" which implied that they could take it with them. This is obviously a mistake and is easy to change.
- The printed ballot jammed. This caused the machine to be taken out of service until the problem was corrected. In order to remove the jammed ballots they had to be extracted with whatever tools were on hand at the early voting sites. A backscratcher and a windshield wiper, for example, were used.
- Voters complained that the printed copy of the ballot was hard to read because of the size and lightness of the print and because of the location of the shield which protected the printed copy. These problems are easy to correct. Voters also complained that the length of the ballot made it difficult to check, which will continue to be a problem where the ballot is long.
- Voters wanted to remove the printed ballot to check it before it went back in the machine. This is not possible, of course, because the voter could then remove the ballot without being detected.
- Some voters were concerned that other voters could see his or her ballot. This was a placement problem that can be corrected.
- The location of the shield that protected the printed ballot also made it difficult for a seated voter to see his or her ballot. Again, this is fairly easy to correct.
- The storage area for the printed ballots was too small and needed to be emptied during the day. This is obviously unacceptable and must be corrected.
- After the voter verified his or her ballot on the screen, the printed version was produced. If the voter changed his or her mind, or didn't agree with what was printed, it was too late to correct. This has been corrected but is still potentially problematic. Only ballots approved by the voter should be counted, but at the same time, there must be no way to connect a ballot with a specific voter.

During the canvass of the vote, we manually recounted one of the early voting polling places. The precinct selected included 114 ballots. Because of the complexity of the ballot and the fact that there were 246 ballot types, it took 127.5 hours to recount. The machine count and count of the paper ballots matched exactly.

Following this demonstration project, Avante made numerous changes to the equipment, addressing most if not all of the concerns expressed.

In conclusion, while a voter verified paper audit trail may increase voter's confidence in the use of an electronic ballot, it is not without concern.

While many of the concerns that I have identified can and have been resolved, there remain concerns that may not be fixable. For example, at the polling place the problem with fleeing voters, printer jams, and the length of time necessary for a voter to verify his or her ballot. After the election there would be significant delays providing official election results from a manual count of paper ballots in case of recount or challenged election. These issues remain unresolved.

I'll be happy to try to respond to any questions that you have.



COUNTY OF SACRAMENTO VOTER REGISTRATION AND ELECTIONS

We proudly conduct elections with accuracy, integrity and dignity.

ERNEST R. HAWKINS
Director

JILL LAVINE
Assistant Director

AL FAWCETT
Administrative Services Officer

Date: November 15, 2002
To: Bob Jennings, Chairman
Voting Systems and Procedure Panel
From: Ernie Hawkins, Registrar of Voters Sacramento County
Re: Early Voting using the Avante System

At the Voting System Panel meeting on October 11, 2002, the Avante System was certified for use in Early Voting in Sacramento County. The Panel requested that Sacramento County prepare a report of their experience using the Avante System. The following are comments and observations made by the County's staff. From our point of view, Early Voting with the Avante system was a success. Sacramento County learned a great deal and enjoyed the experience even though it was very taxing on the staff. The Avante system met our requirements and expectations.

Overview

The Avante personnel were great to work with, despite cutting it close with promised deadlines, they were always there when we needed them. They listened to our suggestions and responded to all our needs. They all have a great "can do" attitude.

Sacramento County had a problem with the programming of the ballot layout. Avante was able to understand the problem, fix it and make it work on their system, with the results being a seamless transfer of data from their system to ours.

Avante provided each of the Early Voting sites with their best IT staff. Avante personnel knew their system and worked well with the County's staff. They were responsive to any needs and assisted in all phases of the Early Voting process.

3700 BRANCH CENTER ROAD, SACRAMENTO, CALIFORNIA 95827-3808
TELEPHONE: (916) 875-6451 FAX: (916) 875-6516 TOLL FREE: (800) 762-8019
SPEECH AND HEARING IMPAIRED - CALIFORNIA RELAY SERVICE (TTY) 1-800-735-2929

Voters with Disabilities

One of the concerns with the Avante system was how a voter in a seated position, such as a wheel chair, would be able to see the screen and vote. There were two solutions offered. One was to use the curbside voting device. This unit was placed in the voter's lap. The second option was an adjustable table. Avante had ordered the adjustable tables but they proved not to be suitable for the weight of the voting units. None of the Early Voting Sites had an adjustable table.

The visually impaired voters were excited about being able to vote by themselves with no assistance. At Market Square, due to the surrounding noise, a visually impaired voter had difficulty with the headphones. These headphones should be replaced with "External Noise Isolation Head Phones". The pivoting earpiece covers the entire ear, blocking out external noise.

The voters with mobility disabilities were pleased with the ease of voting.

Printed Record

The Avante system produces a printed record. Adding a printer and paper to the voting process was a challenge. It was new for the voter and some did not even want to see the printed record. Some voters liked the option of reviewing the printed record, some did not care and some did not want to take the extra seconds to see it. It was confusing for some because they thought they could take it with them. If Avante continues using the printed record, they need to use something other than the word "receipt". It is a print out of the voter's ballot, when we use the term "receipt" voters think of it as the stub they receive at the polls.

If the printed record jams, the machine is out of service until someone can take care of the problem. We relied on the Avante staff to take care of this problem. A few times when the printed record stuck they had to be extracted with many creative tools that were on hand at the early voting site such as a windshield wiper or a back scratcher. Procedures need to be in place for the handling of the printed record in these types of occurrences.

The voter viewed the printed record through a plastic shield on the front of the machine. Voters complained that it was difficult to read because of the length of the ballot, size and darkness of the print and the location of shield. Most voters wanted to remove the paper copy and check it out before it went back into the machine. If the placement of the printed record is not changed, voting machines need to be spaced apart so that the voter cannot see the printed record of the voter next to them. Another option would be to use opaque sides on the shield.

The location of the shields keeps voters in a seated position from getting close to the machine.

The plastic shields are inserted into slots on front of the machines, and then locked in place for the day. We did have a voter knock off the shield then the

printed record was not retracted into the machine and needed handling by a precinct officer.

There was concern that the machines would have problems storing the voter's printed receipts. It was decided to empty the tray every ten voters. This procedure was stopped. The machines must not be opened during the day to empty the tray.

Avante has several options for the printed receipt. The option used for Early Voting was the receipt was a print out of what the voter had selected. Any changes had to be done at the time the voter reviewed their ballot on screen, before selecting the cast ballot button. If the voter did not agree with what they saw it was too late, the ballot was cast.

The other option, which was not used, was for the voter to review the printed receipt then they could accept or make changes. There was concern about the amount of paper that would be used and the possibility of unnecessary printer jamming. In addition, there must be some way to mark the ballot that is ultimately approved by the voter in order to insure that a voter does not cast multiple votes. Any such markings must not give the voter the impression that his ballot can be identified.

Canvass

One of the Avante features is a public and protective counter. This counter shows how many votes have been cast on the machine for the election, and total votes cast on the machine. The counters advanced when a vote was recorded. In addition the counter advanced by one each day when the machine was opened and the printout was done. This gave misleading "vote" counts on the machine.

Processing the Provisional votes was a very quick and easy process. After office staff verified the eligibility of the voter, the Provisional envelope was opened and the ballot card was loaded into the machine for counting.

Avante's report for write-in candidates contained the name of each person that was written in, regardless if they were a certified candidate or not. Since over voting is impossible, this system makes the canvass of the write-ins go much faster.

As part of the certification, we were asked to include one of the Early Voting sites in our one percent manual tally. The Secretary of State's Archive Site was selected. We verified the number of voters on one machine with the report printed out. We verified the report with the paper record and then we verified the machine totals with the paper record. We learned that a fleeing voter has no paper record, for privacy reasons, therefore when counting the voter receipts with the printout you must confirm the number of voters and check the activity log print out for the fleeing voters. All counts balanced.

Early Voting sites include all voting precincts in the County so the manual tally included all contests in the County. To recount the one machine, 114 voters, it took 127.5 hours. While this is not an Avante specific problem, it is an Early Voting problem and this procedure will need to be studied.

Set-up/tear down

There were some concerns from the Precinct Officers that worked the Early Voting sites about the weight and size of the machine. Depending on the site, securing the systems every evening took from 15 minutes to 45 minutes. The units were cumbersome so carts were used to move them.

Voter's Comments

The Voters especially liked the capability of voting any ballot style at any Early Voting Site. Having both the English and Spanish language on the units was very important to some voters.

The number of voters exposed to early voting far exceeded the actual counts of ballots voted and demonstrated. The system is very easy to vote on, intuitive if a person has any Windows experience at all (scroll, review, etc), and easy to pick up with just the video demonstration and one pass on the demo machine.

The voters wanted more privacy around the machines. This may be due to the public settings of the voting site. It is not very private in a busy mall.

Another concern was the sensor. When the voter had a question and stepped away from the machine, the voting page closed and another card had to be created for them. If this were a fleeing voter, you would want the page to close. The timer on the sensor may need to be adjusted. Avante was always there to help.

The main comment from the voters was that a flashing notice came up on the screen telling them to make their selection. It would appear in the middle of the screen over the contest, so the voter could not read what the choices were. They wanted more time before this notice appeared or do away with it altogether. There was not enough time to read the lengthy Propositions. Voters would like their selection to light up before the screen goes onto the next contest so they can verify, at that time, they voted for the candidate or issue of their choice.

The staff that proofed the ballots (screen prints) would have liked to see an actual ballot displayed on the Avante unit. If they had noticed any timing problems, this could be adjusted while in the process of programming.

At first, there was no scroll bar on the demo machine so we could not show voters how and where to scroll. On the actual voting machines the scroll bar was on the left of the screen and most of the voters are used to the scroll bar being on the right side.

When there is a "vote for no more than five" on the ballot the demonstration needs to show the voter that if they vote for less than five they need to be instructed to "skip contest" for the candidates they do not want to vote for.

Avante immediately made modification to the voting program on their Demo units as problems arose. They were not able to make any corrections on the units used during the early voting period because of the security of the ballot but did note all of our requests for changes.

Conclusion

Sacramento County election staff was very satisfied with the results of early voting. We enjoyed working with Avante. The voters were very eager to use the new voting system. It was very gratifying to observe the voters with disabilities and the visually impaired vote for the first time in their life. A voter with no apparent disability requested the headset to vote. His parents accompanying him were ecstatic that he was able to vote. His problem was he could not read. Many times, we expect to visually be aware of a disability, this is not always true.

November 14, 2002

BY HAND DELIVERY

Robert Jennings
Undersecretary of State and Chair of
Voting Systems Panel
California Secretary of State
1500 11th Street
Sacramento, CA 95814

Re: Approval of Avante VOTE-TRAKKER™, Model No. EVC308

Dear Mr. Jennings:

Thank you for arranging the December 2, 2002 meeting of the Voting Systems Panel to consider statewide certification of the Avante VOTE-TRAKKER™ EVC308. Based on the request from you dated November 1, 2002, we have assembled and enclosed the following reports for the Panel:

- ◆ Report on the results of the system test in Sacramento County (Attachment A)
- ◆ Report on the results of the voter and poll worker surveys (Attachment B)

You also requested a report on any problems or issues with the VOTE-TRAKKER™ system in any jurisdiction. We have nothing to report in this area because the system has not been used in any vote other than Sacramento County.

We understand that Sacramento County will submit a separate report to the Panel on its experience with the VOTE-TRAKKER™.

We are pleased to report that the early voting in Sacramento County was successful. Our system was 100 percent accurate in recording voter intent, with zero percent residual votes. Provisional voters were able to participate and their votes will be counted fully once their voting status has been confirmed.

The feedback we received from voters and poll workers was positive and we can address most of the issues raised through simple setting or programming changes.

We note the following highlights from Attachments A and B:

1. A total of 1,612 valid ballots were cast in the early voting as compared with 275,487 ballots in the county's ordinary, punch-card vote.

2. There were 100 provisional votes in the early voting. This occurred when the poll worker could not locate a voter's name in the registration database. All provisional votes were recorded electronically. The county reports that 88 of the 100 provisional votes have been validated and are included in the total of 1,612 valid ballots cast.
3. A total of nine visually impaired voters used the voice-assistance provision. Several wheelchair users voted without difficulty. There were 10 voters who used the Spanish alternative language for voting.
4. There were approximately 20 "fleeing voters" (1.2%), i.e., voters who stepped away before completing their votes. Whatever selections they made were cast and counted 100% correctly. Some of the "fleeing voters" finished their votes, with poll worker assistance, after their initial ballots were spoiled and they re-voted.
5. Voter intent as to every single ballot was resolved. That is, there are zero residual votes. Voters who chose to not to vote on a contest signaled their intent by pressing on the button marked "Skip Contest (No Vote)".
6. In the contests for statewide officeholders, there were substantially fewer under votes in the early voting than in the county's punch card voting.
7. **VOTERS' COMMENTS AND SURVEY:** More than 90% of the voters thought the system was "great" with only 7% evaluating it as "so-so". Less than 2.2% of the voters thought the system needed additional work. Most of the comments involved the prompt ("please make your selection"). We set the machines so that 10 seconds would pass before the prompt appeared, but that time period was too short for many voters. Another major comment was that we should provide numbering next to the candidates to conform to the punch-card system.
8. **POLL WORKERS' SURVEY AND COMMENTS:** Of the 18 poll workers who responded, the responses have been predominantly positive (please refer to the "Poll Worker Questionnaire Section"). The responses may be summarized as follows:
 - ✓ System was easy to use, and set-up time ranged from a few minutes to an hour.
 - ✓ The electronic provisional voting process was easy and simple.
 - ✓ Language selection (English or Spanish) was good and easy.
 - ✓ Vendor assistance was good to great.
 - ✓ Closing the poll each day was easy and OK.
 - ✓ Programming the ballot access smart card was not a problem.
 - ✓ Working with laptops to issue ballot access cards and look up voter registration was good to great.

- ✓ Printed receipts were good. The voters seemed to like them. Some voters voiced that they would like a copy.
- ✓ Most had no problem emptying paper trays.
- ✓ The system procedures were good and needed no changes.

Based on the suggestions from the voters, we will modify the programming or settings of the VOTE-TRAKKER™ as follows:

- ✓ We will change the default on the prompt (“please make your selection”) so that it will not appear for at least 30 seconds, even for the most simple contests. For complex contests, the time will lengthen automatically depending on the complexity of the question. Also, the prompt will appear on the top portion of the screen, away from the contests, so it is less distracting. Counties may choose to omit the prompt altogether, or they can lengthen the time before the prompt appears.
- ✓ So as to make it clearer to voters that their votes are registering, the selections they make will be highlighted on the screen for 0.3 second, also adjustable by the jurisdiction, instead of the millisecond that was used during the Sacramento County early voting.
- ✓ We will move the scroll bar to the right side of the screen to make it more visible.
- ✓ The viewing window will be changed in material to include anti-static properties to prevent the paper from “sticking” to the walls of the window.

We will demonstrate these improvements at the meeting of the Panel on December 2.

With regard to the percentage of under-votes, the VOTE-TRAKKER™ compared favorably to the punch-card system used on election day in Sacramento. In Attachment C, we offer both bar and pie charts demonstrating that the VOTE-TRAKKER™ achieved a lower percentage of under-votes (intentional) with 0% residual votes when compared with the cumulative votes combining punch card votes and early voting votes.

At the October 11, 2002 meeting, the Panel discussed the weight and portability of the VOTE-TRAKKER™ EVC 308 units. Since their weight is 44 to 52 pounds per unit, depending on the paper that is loaded, this should not pose a problem as demonstrated in the Sacramento Early Voting.

However, while we believe that some jurisdictions will prefer the single module design of the EVC 308, we separately will propose the certification of an

alternative system, the EVC 328, which separates the printer and paper from the rest of the unit. The printer module on the EVC 328 will have a built-in viewing window that can be tilted to the eye level of the voters for easier reading. The font size will be larger and easier to read. The printer and voting modules on the EVC 328 each will be substantially lighter than 44 pounds (20-22 pounds each, please refer to Attachment D).

Concerning our ability to interface with existing reporting and ballot management software, we were able to interface with DFM's reporting software successfully. In fact, Avante staff was able to create, test, and implement the interface in less than one week. Sacramento IT staff were pleased with the speed and effectiveness of our programming staff. Avante even solved a database conflict that was discovered in the ballot layout software used by the county.

Finally, you asked us to communicate with Robert Naegele of Granite Creek Technology regarding the procedures we submitted for the VOTE-TRAKKER™ EVC 308. We have submitted revised procedures, which we understand are acceptable to both Mr. Naegele and to Dawn Mehlhaff of your staff. We look forward to the meeting on December 2. In the meantime, please let me or my staff know if the Panel needs any additional information.

Sincerely yours,

Kevin Chung, Ph.D.
President and CEO of AVANTE International Technology, Inc. and
AI Technology, Inc.
70 Washington Road, Princeton Junction, NJ 08550
Tel: (609) 799-9388

ATTACHMENT A

SUMMARY OF SEMIFINAL TALLIES FROM EARLY VOTING

The following pages are tabulations of the SEMIFINAL OFFICIAL RESULTS for the EARLY VOTING of Sacramento, CA. In some typical statewide elections, comparative analysis has been posted from the SEMIFINAL OFFICIAL CUMULATIVE RESULTS of the complete November 5, 2002 election for the County.

The following aspects should be emphasized:

1. The results are not final and must be confirmed by final canvassing of the county.
2. Some of the statewide county cumulative results have been incorporated for comparison purposes only.
3. While the results on residual votes may be a good indication of the error-free nature of VOTE-TRAKKER™ system, the higher rate of under-votes with the use of punch-card system may also reflect the more “educated” voters that the early voting tends to attract.
4. There were six locations each holding voting sessions for eleven days. Each machine was suspended at the end of the day and started-up again every morning by the poll workers.
5. There are total of six groups of poll workers along with a county staff and an AVANTE staff for each location.

General Election November 5, 2002
Sacramento, CA: SEMIFINAL OFFICIAL RESULTS
 (11/06/2002)

Tally Type: Normal, Provisional Result Type: EARLY VOTING
 Voting System: VOTE-TRAKKER™ DRE Touch-Screen

State Governor State: CA
 Ballot Cast: 1612 Skip Contest (No Vote): 25 Write-In: 20

Candidate/ Write-In	Number Voted	Percentage	Party
GRAY DAVIS	729	45.22%	Democratic
BILL SIMON	605	37.53%	Republican
PETER MIGUEL CAMEJO	160	9.93%	Green
GARY DAVID COPELAND	30	1.86%	Libertarian
IRIS ADAM	23	1.43%	Natural Law
REINHOLD GULKE	20	1.24%	American Independent
Richard RIORDAN	10	0.62%	
Richard D. DEPAOLA	1	0.06%	
Rodney K. AOKI	1	0.06%	
Steven HORN	1	0.06%	
Ray CASE	1	0.06%	
Mickey MOUSE	1	0.06%	
Dusty BAKER	1	0.06%	
Bill JONES	1	0.06%	
Arnold SWARTZENAGGER	2	0.12%	
Tiger SULLIVAN	1	0.06%	
Intentional Undervote (Skip Contest)	25	1.55%	
Unintentional Undervote	0	0.00%	
Total	1612	100%	

Tally Type: Normal, Provisional Result Type: CUMULATIVE TOTALS
 Voting System: Punch-card

State Governor State: CA
 Ballot Cast: 275,487 Under Votes: 10,201 Over Votes: 813

Candidate/ Write-In	Number Voted	Percentage	Party
GRAY DAVIS	109,908	39.90%	Democratic
BILL SIMON	121,087	43.95%	Republican
PETER MIGUEL CAMEJO	18,744	6.80%	Green
GARY DAVID COPELAND	5,601	2.03%	Libertarian
IRIS ADAM	3,866	1.40%	Natural Law
REINHOLD GULKE	5,267	1.91%	American Independent
Write-In Candidates			
Intentional + Unintentional Under Votes (Un-resolved)	10,201	3.70%	
Total	275,487	100%	

Tally Type: Normal, Provisional Result Type: EARLY VOTING
 Voting System: VOTE-TRAKKER™ DRE Touch-Screen

=====
Secretary of State State: CA
 Ballot Cast: 1612 Skip Contest (Skip Contest (No Vote)): 53 Write-In: 0

Candidate/ Write-In	Number Voted	Percentage	Party
KEVIN SHELLEY	703	43.61%	Democratic
KEITH OLBERG	627	38.90%	Republican
LARRY SHOUP	91	5.66%	Green
LOUISE MARIE ALLISON	58	3.60%	Natural Law
GAIL K. LIGHTFOOT	41	2.54%	Libertarian
EDWARD C. NOONAN	28	1.74%	American Independent
VALLI SHARPE-GEISLER	11	0.68%	Reform
Intentional Undervote (Skip Contest)	53	3.29%	
Unintentional Undervote	0	0.00%	
Total	1612	100%	

Tally Type: Normal, Provisional Result Type: CUMULATIVE TOTALS
 Voting System: Punch-card

=====
 Contest Position: Secretary of State State: CA
 Ballot Cast: 275,487 Under Votes: 15,819 Over Votes: 514

Candidate/ Write-In	Number Voted	Percentage	Party
KEVIN SHELLEY	112,902	40.98%	Democratic
KEITH OLBERG	116,659	42.35%	Republican
LARRY SHOUP	10,281	3.73%	Green
LOUISE MARIE ALLISON	6,363	2.31%	Natural Law
GAIL K. LIGHTFOOT	6,943	2.52%	Libertarian
EDWARD C. NOONAN	3,430	1.25%	American Independent
VALLI SHARPE-GEISLER	2,576	0.68%	Reform
Write-In Candidates			
Intentional + Unintentional Under Votes (Un-resolved)	15,819	5.74%	
Total	275,487	100%	

Tally Type: Normal, Provisional Result Type: EARLY VOTING
 Voting System: VOTE-TRAKKER™ DRE Touch-Screen

=====
State Attorney General State: CA
 Ballot Cast: 1612 Skip Contest (Skip Contest (No Vote)): 29 Write-In: 0

Candidate/ Write-In	Number Voted	Percentage	Party
BILL LOCKYER	884	54.84%	Democratic
DICK ACKERMAN	543	33.68%	Republican
GLEN FREEMAN MOWRER	79	4.90%	Green
DIANE BEALL TEMPLIN	53	3.29%	American Independent
ED KUWATCH	24	1.49%	Libertarian
Intentional Undervote	29	1.80%	
Unintentional Undervote	0	0.00%	
Total	1612	100%	

Tally Type: Normal, Provisional Result Type: CUMULATIVE TOTALS
 Voting System: Punch-card

=====
State Attorney General State: CA
 Ballot Cast: 275,487 Under Votes: 15,265 Over Votes: 933

Candidate/ Write-In	Number Voted	Percentage	Party
BILL LOCKYER	130,351	47.32%	Democratic
DICK ACKERMAN	107,526	39.03%	Republican
GLEN FREEMAN MOWRER	9,857	3.58%	Green
DIANE BEALL TEMPLIN	7,790	2.83%	American Independent
ED KUWATCH	3,765	1.37%	Libertarian
Write-In Candidates			
Intentional + Unintentional Under Votes (Un-resolved)	15,265	5.54%	
Total	275,487	100%	

Tally Type: Normal, Provisional Result Type: EARLY VOTING
 Voting System: VOTE-TRAKKER™ DRE Touch-Screen

=====
State Insurance Commissioner State: CA
 Ballot Cast: 1612 Skip Contest (Skip Contest (No Vote)): 57 Write-In: 0

Candidate/ Write-In	Number Voted	Percentage	Party
JOHN GARAMENDI	782	48.51%	Democratic
GARY MENDOZA	608	37.72%	Republican
DAVID I. SHEIDLOWER	78	4.84%	Green
STEVE KLEIN	30	1.86%	American Independent
RAUL CALDERON JR.	29	1.80%	Natural Law
DALE F. OGDEN	28	1.74%	Libertarian
Intentional Undervote	57	3.53%	
Unintentional Undervote	0	0.00%	
Total	1612	100%	

Tally Type: Normal, Provisional Result Type: CUMULATIVE TOTALS
 Voting System: Punch-card

=====
State Insurance Commissioner State: CA
 Ballot Cast: 275,487 Under Votes: 17,186 Over Votes: 757

Candidate/ Write-In	Number Voted	Percentage	Party
JOHN GARAMENDI	111,165	40.35%	Democratic
GARY MENDOZA	117,963	42.82%	Republican
DAVID I. SHEIDLOWER	10,099	3.67%	Green
STEVE KLEIN	5,470	1.99%	American Independent
RAUL CALDERON JR.	5,607	1.80%	Natural Law
DALE F. OGDEN	7,240	2.62%	Libertarian
Write-In Candidates			
Intentional + Unintentional Under Votes (Un-resolved)	17,186	6.24%	
Total	275,487	100%	

Tally Type: Normal, Provisional Result Type: EARLY VOTING
 Voting System: VOTE-TRAKKER™ DRE Touch-Screen

=====
Member, State Board of Equalization, District 2 State: CA

Ballot Cast: 1612 Skip Contest ((No Vote): 94 Write-In: 2

Candidate/ Write-In	Number Voted	Percentage	Party
TOM Y. SANTOS	820	50.87%	Democratic
BILL LEONARD	696	43.18%	Republican
Jan BERGERON (Yes)	1	0.06%	
Ronald REAGAN (Yes)	1	0.06%	
Intentional Undervote	94	5.83%	
Unintentional Undervote	0	0.00%	
Total	1612	100%	

Tally Type: Normal, Provisional Result Type: CUMULATIVE TOTALS
 Voting System: Punch-card

=====
Member, State Board of Equalization, District 2 State: CA

Ballot Cast: 275,487 Under Votes: 40,090 Over Votes: 133

Candidate/ Write-In	Number Voted	Percentage	Party
TOM Y. SANTOS	111,761	40.57%	Democratic
BILL LEONARD	123,503	44.83%	Republican
Write-In Candidates			
Intentional + Unintentional Under Votes (Un-resolved)	40,090	14.55%	
Total	275,487	100%	

Tally Type: Normal, Provisional Result Type: EARLY VOTING
 Voting System: VOTE-TRAKKER™ DRE Touch-Screen

=====
Associate Justice of the Supreme Court (2102) State: CA
 Ballot Cast: 1612 Skip Contest (No Vote): 276 Write-In: 0

Candidate/ Write-In	Number Voted	Percentage	Party
Carlos R. Mareno Yes	1050	65.14%	Non-Partisan
Carlos R. Mareno No	286	17.74%	Non-Partisan
Intentional Undervote	276	17.12%	
Unintentional Undervote	0	0.00%	
Total	1612	100%	

Tally Type: Normal, Provisional Result Type: CUMULATIVE TOTALS
 Voting System: Punch-card

=====
Associate Justice of the Supreme Court (2102) State: CA
 Ballot Cast: 275,487 Under Votes: 92,387 Over Votes: 220

Candidate/ Write-In	Number Voted	Percentage	Party
Carlos R. Mareno Yes	133,509	48.46%	Non-Partisan
Carlos R. Mareno No	49,371	18.92%	Non-Partisan
Intentional + Unintentional Under Votes (Un-resolved)	93,387	33.90%	
Total	275,487	100%	

=====
Contest Position: Associate Justice of the Supreme Court (2105) State: CA
Ballot Cast: 1612 Skip Contest (No Vote): 309 Write-In: 0

Candidate/ Write-In	Number Voted	Percentage	Party
Yes	1017	63.09%	Non-Partisan
No	286	17.74%	Non-Partisan
Intentional Undervote	309	19.17%	
Unintentional Undervote	0	0.00%	
Total	1612	100%	

=====
Contest Position: Associate Justice of the Supreme Court (2107) State: CA
Ballot Cast: 1612 Skip Contest (No Vote): 307 Write-In: 0

Candidate/ Write-In	Number Voted	Percentage	Party
Yes	1052	65.26%	Non-Partisan
No	253	15.69%	Non-Partisan
Intentional Undervote	307	19.05%	
Unintentional Undervote	0	0.00%	
Total	1612	100%	

=====
Contest Position: Presiding Justice, Court of Appeal, Third Appellate District State: CA
Ballot Cast: 1612 Skip Contest (No Vote): 344 Write-In: 0

Candidate/ Write-In	Number Voted	Percentage	Party
Yes	994	61.66%	Non-Partisan
No	274	17.00%	Non-Partisan
Intentional Undervote	344	21.34%	
Unintentional Undervote	0	0.00%	
Total	1612	100%	

=====
Contest Position: Associate Justice, Court of Appeal, Third Appellate District (2204) State: CA
Ballot Cast: 1612 Skip Contest (No Vote): 353 Write-In: 0

Candidate/ Write-In	Number Voted	Percentage	Party
Yes	985	61.10%	Non-Partisan
No	274	17.00%	Non-Partisan
Intentional Undervote	353	21.90%	
Unintentional Undervote	0	0.00%	
Total	1612	100%	

=====

Associate Justice, Court of Appeal, Third Appellate District (2207) State: CA
 Ballot Cast: 1612 Skip Contest (No Vote): 363 Write-In: 0

Candidate/ Write-In	Number Voted	Percentage	Party
Yes	968	60.05%	Non-Partisan
No	281	17.43%	Non-Partisan
Intentional Undervote	363	22.52%	
Unintentional Undervote	0	0.00%	
Total	1612	100%	

=====

Associate Justice, Court of Appeal, Third Appellate District (2208) State: CA
 Ballot Cast: 1612 Skip Contest (No Vote): 359 Write-In: 0

Candidate/ Write-In	Number Voted	Percentage	Party
Yes	994	61.66%	Non-Partisan
No	259	16.07%	Non-Partisan
Intentional Undervote	359	22.27%	
Unintentional Undervote	0	0.00%	
Total	1612	100%	

=====

Associate Justice, Court of Appeal, Third Appellate District (2209) State: CA
 Ballot Cast: 1612 Skip Contest (No Vote): 358 Write-In: 0

Candidate/ Write-In	Number Voted	Percentage	Party
Yes	970	60.17%	Non-Partisan
No	284	17.62%	Non-Partisan
Intentional Undervote	358	22.21%	
Unintentional Undervote	0	0.00%	
Total	1612	100%	

=====

Associate Justice, Court of Appeal, Third Appellate District (2210) State: CA
 Ballot Cast: 1612 Skip Contest (No Vote): 333 Write-In: 0

Candidate/ Write-In	Number Voted	Percentage	Party
Yes	1010	62.66%	Non-Partisan
No	269	16.69%	Non-Partisan
Intentional Undervote	333	20.65%	
Unintentional Undervote	0	0.00%	
Total	1612	100%	

=====
State Superintendent of Public Instruction State: CA
Ballot Cast: 1612 Skip Contest (No Vote): 155 Write-In: 0

Candidate/ Write-In	Number Voted	Percentage	Party
JACK O'CONNELL	901	55.89%	Non-Partisan
KATHERINE H. SMITH	556	34.49%	Non-Partisan
Intentional Undervote	155	9.62%	
Unintentional Undervote	0	0.00%	
Total	1612	100%	

Tally Type: Normal, Provisional Result Type: EARLY VOTING
 Voting System: VOTE-TRAKKER™ DRE Touch-Screen

=====
United States Representative, Congressional District 3 State: CA County: Sacramento
Ballot Cast: 772 Skip Contest (No Vote): 15 Write-In: 1

Candidate/ Write-In	Number Voted	Percentage	Party
DOUG OSE	443	57.38%	Republican
HOWARD BEEMAN	286	37.05%	Democratic
DOUGLAS ARTHUR TUMA	27	3.50%	Libertarian
Paul A. JOHNSON (Yes)	1	0.13%	
Intentional Undervote	15	1.94%	
Unintentional Undervote	0	0.00%	
Total	772	100%	

Tally Type: Normal, Provisional Result Type: CUMULATIVE TOTALS
 Voting System: Punch-card

=====
United States Representative, Congressional District 3 State: CA County: Sacramento
Ballot Cast: 275,487 Under Votes: 11,735 Over Votes: 121

Candidate/ Write-In	Number Voted	Percentage	Party
DOUG OSE	84,577	57.71%	Republican
HOWARD BEEMAN	46,189	31.73%	Democratic
DOUGLAS ARTHUR TUMA	4,044	2.76%	Libertarian
Intentional + Unintentional Under Votes (Un-resolved)	11,735	8.01%	
Total	146,545	100%	

=====
United States Representative, Congressional District 4 State: CA County: Sacramento
Ballot Cast: 43 Skip Contest (No Vote): 1 Write-In: 0

Candidate/ Write-In	Number Voted	Percentage	Party
JOHN T. DOOLITTLE	28	65.12%	Republican
MARK A. NORBERG	10	23.26%	Democratic
ALLEN M. ROBERTS	4	9.30%	Libertarian
Intentional Undervote	1	2.32%	
Unintentional Undervote	0	0.00%	
Total	43	100%	

=====
United States Representative, Congressional District 5 State: CA County: Sacramento
Ballot Cast: 795 Skip Contest (No Vote): 25 Write-In: 0

Candidate/ Write-In	Number Voted	Percentage	Party
ROBERT T. MATSUI	567	71.32%	Democratic
RICHARD FRANKHUIZEN	164	20.63%	Republican
TIMOTHY E. ROLOFF	39	4.91%	Libertarian
Intentional Undervote	25	3.14%	
Unintentional Undervote	0	0.00%	
Total	795	100%	

=====
United States Representative, Congressional District 10 State: CA County: Sacramento
Ballot Cast: 2 Skip Contest (No Vote): 0 Write-In: 0

Candidate/ Write-In	Number Voted	Percentage	Party
ELLEN O. TAUSCHER	2	100.00%	Democratic
SONIA E. ALONSO HARDEN	0	0.00%	Libertarian
Intentional Undervote	0	0.00%	
Unintentional Undervote	0	0.00%	
Total	2	100%	

Tally Type: Normal, Provisional Result Type: EARLY VOTING
 Voting System: VOTE-TRAKKER™ DRE Touch-Screen

=====
State Senator, Senate District 6 State: CA County: Sacramento
 Ballot Cast: 1035 Skip Contest (No Vote): 75 Write-In: 19

Candidate/ Write-In	Number Voted	Percentage	Party
DEBORAH ORTIZ	705	68.11%	Democratic
JASON A. SEWELL	236	22.80%	Libertarian
Yolanda KNAACK (Yes)	16	1.55%	
Homer SIMPSON (Yes)	1	0.10%	
Yolanda KNAAP (Yes)	1	0.10%	
Yolanda KNACK (Yes)	1	0.10%	
Intentional Undervote	75	7.24%	
Unintentional Undervote	0	0.00%	
Total	1035	100%	

Tally Type: Normal, Provisional Result Type: EARLY VOTING
 Voting System: VOTE-TRAKKER™ DRE Touch-Screen

=====
State Senator, Senate District 6 State: CA County: Sacramento
 Ballot Cast: 164,559 Under Votes: 21,122 Over Votes: 98

Candidate/ Write-In	Number Voted	Percentage	Party
DEBORAH ORTIZ	104,436	63.46%	Democratic
JASON A. SEWELL	39,001	23.70%	Libertarian
Write-Ins			
Intentional + Unintentional Under Votes (Un-resolved)	21,122	12.83%	
Total	164,559	100%	

=====
Member, State Assembly, District 4 State: CA County: Sacramento
Ballot Cast: 55 Skip Contest (No Vote): 1 Write-In: 0

Candidate/ Write-In	Number Voted	Percentage	Party
SCOTT WARREN	28	50.91%	Democratic
TIM LESLIE	26	47.27%	Republican
Intentional Undervote	1	1.82%	
Unintentional Undervote	0	0.00%	
Total	55	100%	

=====
Member, State Assembly, District 5 State: CA County: Sacramento
Ballot Cast: 583 Skip Contest (No Vote): 13 Write-In: 0

Candidate/ Write-In	Number Voted	Percentage	Party
DAVE COX	335	57.46%	Republican
ERIC ULIS	203	34.82%	Democratic
ROBERTO LEIBMAN	32	5.49%	Libertarian
Intentional Undervote	13	2.23%	
Unintentional Undervote	0	0.00%	
Total	583	100%	

=====
Member, State Assembly, District 9 State: CA County: Sacramento
Ballot Cast: 535 Skip Contest (No Vote): 18 Write-In: 1

Candidate/ Write-In	Number Voted	Percentage	Party
DARRELL STEINBERG	383	71.59%	Democratic
DAVID A. PEGOS	106	19.81%	Republican
DOUGLAS M. POSTON	27	5.05%	Libertarian
Grantland JOHNSON (Yes)	1	0.19%	
Intentional Undervote	18	3.36%	
Unintentional Undervote	0	0.00%	
Total	535	100%	

=====
Member, State Assembly, District 10 State: CA County: Sacramento
Ballot Cast: 347 Skip Contest (No Vote): 14 Write-In: 0

Candidate/ Write-In	Number Voted	Percentage	Party
KATHERINE E. MAESTAS	178	51.30%	Democratic
ALAN NAKANISHI	155	44.67%	Republican
Intentional Undervote	14	4.03%	
Unintentional Undervote	0	0.00%	
Total	347	100%	

=====
Member, State Assembly, District 15 State: CA County: Sacramento
Ballot Cast: 92 Skip Contest (No Vote): 5 Write-In: 0

Candidate/ Write-In	Number Voted	Percentage	Party
GUY HOUSTON	55	59.78%	Republican
DONNA GERBER	32	34.78%	Democratic
Intentional Undervote	5	5.44%	
Unintentional Undervote	0	0.00%	
Total	92	100%	

=====
Los Rios Community College District, Governing Board Member-Area 6 State: CA County: Sacramento
Ballot Cast: 334 Skip Contest (No Vote): 64 Write-In: 0

Candidate/ Write-In	Number Voted	Percentage	Party
BRUCE POMER	179	53.59%	Non-Partisan
BRUCE FARHANGI	57	17.07%	Non-Partisan
DARROW SPRAGUE	34	10.18%	Non-Partisan
Intentional Undervote	64	19.16%	
Unintentional Undervote	0	0.00%	
Total	334	100%	

=====
San Joaquin Delta Community College District, Governing Board Member-Area 3 State: CA County: Sacramento
Ballot Cast: 11 Skip Contest (No Vote): 3 Write-In: 0

Candidate/ Write-In	Number Voted	Percentage	Party
JANET A. RIVERA	7	63.64%	Non-Partisan
WILLIAM GIFFORD	1	9.09%	Non-Partisan
BOB HAILEY	0	0.00%	Non-Partisan
Intentional Undervote	3	27.27%	
Unintentional Undervote	0	0.00%	
Total	11	100%	

=====
San Joaquin Delta Community College District, Governing Board Member-Area 7 State: CA County: Sacramento
Ballot Cast: 11 Skip Contest (No Vote): 3 Write-In: 0

Candidate/ Write-In	Number Voted	Percentage	Party
STEPHEN A. SCHMIEDT	4	36.36%	Non-Partisan
TED SIMAS	4	36.36%	Non-Partisan
Intentional Undervote	3	27.28	
Unintentional Undervote	0	0.00%	
Total	11	100%	

=====

Sierra Community College District, Governing Board Member-Area 2 (Full Term) State: CA County: Sacramento
 Ballot Cast: 23 Skip Contest (No Vote): 4 Write-In: 0

Candidate/ Write-In	Number Voted	Percentage	Party
DAVID FERRARI	15	65.22%	Non-Partisan
MICHAEL T. LIPE	4	17.39%	Non-Partisan
Intentional Undervote	4	17.39%	
Unintentional Undervote	0	0.00%	
Total	23	100%	

=====

Sierra Community College District, Governing Board Member-Area 5 (Full Term) State: CA County: Sacramento
 Ballot Cast: 23 Skip Contest (No Vote): 3 Write-In: 0

Candidate/ Write-In	Number Voted	Percentage	Party
DAVE CREEK	13	56.52%	Non-Partisan
DAN SOKOL	7	30.43%	Non-Partisan
Intentional Undervote	3	13.05%	
Unintentional Undervote	0	0.00%	
Total	23	100%	

=====

Sierra Community College District, Governing Board Member-Area 6 (Full Term) State: CA County: Sacramento
 Ballot Cast: 23 Skip Contest (No Vote): 4 Write-In: 0

Candidate/ Write-In	Number Voted	Percentage	Party
NANCY B. PALMER	11	47.83%	Non-Partisan
JIM PERKINS	4	17.39%	Non-Partisan
DAVID J. HODDER	2	8.70%	Non-Partisan
JAMES A. HINMAN	2	8.70%	Non-Partisan
Intentional Undervote	4	17.38%	
Unintentional Undervote	0	0.00%	
Total	23	100%	

=====

Sierra Community College District, Governing Board Member-Area 4 (Short Term) State: CA County: Sacramento
 Ballot Cast: 23 Skip Contest (No Vote): 4 Write-In: 0

Candidate/ Write-In	Number Voted	Percentage	Party
JIM ROBISON	12	52.17%	Non-Partisan
JERRY SIMMONS	6	26.09%	Non-Partisan
STAN PLUTA	1	4.35%	Non-Partisan
Intentional Undervote	4	17.39%	
Unintentional Undervote	0	0.00%	
Total	23	100%	

Center Unified School District, Governing Board Member State: CA County: Sacramento
 Ballot Cast: 48 Skip Contest (No Vote): 15 Write-In: 0

Candidate/ Write-In	Number Voted	Percentage	Party
KATHY PALMER	8	16.67%	Non-Partisan
NANCY ANDERSON	7	14.58%	Non-Partisan
SCOTT C. RODOWICK	5	10.42%	Non-Partisan
LIBBY ANN WILLIAMS	5	10.42%	Non-Partisan
MARC POVONDRA	5	10.42%	Non-Partisan
CHERYLE GRAY	3	6.25%	Non-Partisan
Intentional Undervote	15	31.25%	
Unintentional Undervote	0	0.00%	
Total	48	100%	

Elk Grove Unified School District, Governing Board Member-Area 2 State: CA County: Sacramento
 Ballot Cast: 285 Skip Contest (No Vote): 35 Write-In: 0

Candidate/ Write-In	Number Voted	Percentage	Party
JEANETTE J. BEACH-BILLINGSLY	116	40.70%	Non-Partisan
JOHN TAYLOR	69	24.21%	Non-Partisan
STEVE LY	65	22.81%	Non-Partisan
Intentional Undervote	35	12.28%	
Unintentional Undervote	0	0.00%	
Total	285	100%	

Elk Grove Unified School District, Governing Board Member-Area 5 State: CA County: Sacramento
 Ballot Cast: 285 Skip Contest (No Vote): 36 Write-In: 0

Candidate/ Write-In	Number Voted	Percentage	Party
PRISCILLA S. COX	182	63.86%	Non-Partisan
DAVIES O. ONONIWU	67	23.51%	Non-Partisan
Intentional Undervote	36	12.63%	
Unintentional Undervote	0	0.00%	
Total	285	100%	

Folsom Cordova Unified School District, Governing Board Member State: CA County: Sacramento
 Ballot Cast: 255 Skip Contest (No Vote): 28 Write-In: 0

Candidate/ Write-In	Number Voted	Percentage	Party
RICHARD SHAW	50	19.61%	Non-Partisan
ED SHORT	42	16.47%	Non-Partisan
HEIDI R. P. KONARSKI	37	14.51%	Non-Partisan
SARA A. MYERS	37	14.51%	Non-Partisan
JIM MC GOWAN	31	12.16%	Non-Partisan
KATE MORRIS	30	11.76%	Non-Partisan
Intentional Undervote	28	10.98 %	
Unintentional Undervote	0	0.00%	
Total	255	100%	

=====

Sacramento City Unified School District, Governing Board Member State: CA County: Sacramento
 Ballot Cast: 1461 Skip Contest (No Vote): 313

Write-In: 1

Candidate/ Write-In	Number Voted	Percentage	Party
ROB FONG	247	16.91%	Non-Partisan
ROY GRIMES	216	14.78%	Non-Partisan
DAWN MC COY	167	11.43%	Non-Partisan
JAMES CRAMER	163	11.16%	Non-Partisan
MARC CARREL	123	8.42%	Non-Partisan
GREGORY J. TATE	85	5.82%	Non-Partisan
LORI POSAS SANTOS	74	5.07%	Non-Partisan
KARI NICHOL LOVE	45	3.08%	Non-Partisan
WARD V. MICKO	27	1.85%	Non-Partisan
Joe JOHNSON (Yes)	1	0.07%	
Intentional Undervote	313	21.43%	
Unintentional Undervote	0	0.00%	
Total	1461	100%	

=====

Contest Position: Galt Joint Union High School District, Governing Board Member State: CA County: Sacramento
 Ballot Cast: 27 Skip Contest (No Vote): 9

Write-In: 0

Candidate/ Write-In	Number Voted	Percentage	Party
BOB ELLIS	6	22.22%	Non-Partisan
DENNIS RICHARDSON	3	11.11%	Non-Partisan
BEN COX JR.	3	11.11%	Non-Partisan
BLAKE RASMUSSEN	3	11.11%	Non-Partisan
PATRICK W. MAPLE	3	11.11%	Non-Partisan
Intentional Undervote	9	33.33%	
Unintentional Undervote	0	0.00%	
Total	27	100%	

=====

Grant Joint Union High School District, Governing Board Member State: CA County: Sacramento
 Ballot Cast: 333 Skip Contest (No Vote): 55

Write-In: 1

Candidate/ Write-In	Number Voted	Percentage	Party
LINDA THOMPSON	55	16.52%	Non-Partisan
ANNETTE EMERY	51	15.32%	Non-Partisan
BRYCE J. VERNON	47	14.11%	Non-Partisan
DARRELL R. NELSON	43	12.91%	Non-Partisan
ERTHIA L. JOHNSON	30	9.01%	Non-Partisan
MICHELLE RIVAS	26	7.81%	Non-Partisan
NETTIE SCOGGINS	25	7.51%	Non-Partisan
Dionne RICH (Yes)	1	0.30%	
Intentional Undervote	55	16.56%	
Unintentional Undervote	0	0.00%	
Total	333	100%	

=====
 Roseville Joint Union High School District, Governing Board Member State: CA County: Sacramento
 Ballot Cast: 14 Skip Contest (No Vote): 2 Write-In: 1

Candidate/ Write-In	Number Voted	Percentage	Party
KELLY L. LAFFERTY	4	28.57%	Non-Partisan
ROSE ANN WERTHEIM	4	28.57%	Non-Partisan
KEN J. ZANOLINI	2	14.29%	Non-Partisan
THOMAS A. BEALE	1	7.14%	Non-Partisan
JAMES JOINER	0	0.00%	Non-Partisan
JASON CARDINET	0	0.00%	Non-Partisan
Kelly LAFFERTY (Yes)	1	7.14%	
Intentional Undervote	2	14.29%	
Unintentional Undervote	0	0.00%	
Total	14	100%	

=====
 Arcohe Union School District, Governing Board Member State: CA County: Sacramento
 Ballot Cast: 0 Skip Contest (No Vote): 0 Write-In: 0

Candidate/ Write-In	Number Voted	Percentage	Party
BECKY VREELAND	0	0%	Non-Partisan
BRENDAN MOORE	0	0%	Non-Partisan
LAURA S. MULROONEY	0	0%	Non-Partisan
LISA M. STEELE	0	0%	Non-Partisan

=====
 Del Paso Heights School District, Governing Board Member State: CA County: Sacramento
 Ballot Cast: 30 Skip Contest (No Vote): 6 Write-In: 6

Candidate/ Write-In	Number Voted	Percentage	Party
CAROLYN A. MOORE	6	20.00%	Non-Partisan
L. LANETTE ROBINSON	5	16.67%	Non-Partisan
ERTHIA L. JOHNSON	4	13.33%	Non-Partisan
HARRY BLOCK	4	13.33%	Non-Partisan
KAI PATHONG VUE	2	6.67%	Non-Partisan
REBECCA UMBLE-MORRIS	2	6.67%	Non-Partisan
MICHAEL P. MC ZEEK SR.	1	3.33%	Non-Partisan
Intentional Undervote	6	20.00%	
Unintentional Undervote	0	0.00%	
Total	30	100%	

=====
 Dry Creek Joint Elementary School District, Governing Board Member State: CA County: Sacramento
 Ballot Cast: 21 Skip Contest (No Vote): 3 Write-In: 0

Candidate/ Write-In	Number Voted	Percentage	Party
WAYNE D. ROBERSON	6	28.57%	Non-Partisan
TRACY PITTMAN	5	23.81%	Non-Partisan
DIANE C. HOWE	3	14.29%	Non-Partisan
GERALD L. GUERRERO	2	9.52%	Non-Partisan
JOSEPH W. ANDROLOWICZ	2	9.52%	Non-Partisan
Intentional Undervote	3	14.29%	
Unintentional Undervote	0	0.00%	
Total	21	100%	

=====

Galt Joint Union Elementary School District, Governing Board Member State: CA County: Sacramento
 Ballot Cast: 27 Skip Contest (No Vote): 1 Write-In: 0

Candidate/ Write-In	Number Voted	Percentage	Party
TINA M. SKINNER	8	29.63%	Non-Partisan
ENRIQUE ZAMORA	7	25.93%	Non-Partisan
DONNA L. FLUTY	7	25.93%	Non-Partisan
DONALD NOTTOLI	4	14.81%	Non-Partisan
Intentional Undervote	1	3.70%	
Unintentional Undervote	0	0.00%	
Total	27	100%	

=====

North Sacramento School District, Governing Board Member State: CA County: Sacramento
 Ballot Cast: 81 Skip Contest (No Vote): 11 Write-In: 0

Candidate/ Write-In	Number Voted	Percentage	Party
ANNE R. PETTIT	16	19.75%	Non-Partisan
MARK F. UNDERWOOD	12	14.81%	Non-Partisan
MIGUEL A. TORRES	12	14.81%	Non-Partisan
VERN L. COLEMAN	11	13.58%	Non-Partisan
CAROL WHEELER	10	12.35%	Non-Partisan
ELIZABETH B. MILLER	9	11.11%	Non-Partisan
Intentional Undervote	11	13.58%	
Unintentional Undervote	0	0.00%	
Total	81	100%	

=====

Rio Linda Union School District, Governing Board Member State: CA County: Sacramento
 Ballot Cast: 192 Skip Contest (No Vote): 42 Write-In: 0

Candidate/ Write-In	Number Voted	Percentage	Party
FREDERICK GAYLE	46	23.96%	Non-Partisan
JANIS R. GREEN	43	22.40%	Green
ELIZABETH (LIZ) MITCHELL	42	21.87%	Non-Partisan
RICHARD LONG	19	9.90%	Non-Partisan
Intentional Undervote	42	21.87%	
Unintentional Undervote	0	0.00%	
Total	192	100%	

=====
City of Folsom, Member City Council **State: CA County: Sacramento**
 Ballot Cast: 105 Skip Contest (No Vote): 8 Write-In: 0

Candidate/ Write-In	Number Voted	Percentage	Party
STEVE FAIRCHILD	18	17.14%	Non-Partisan
STEVE MIKLOS	15	14.29%	Non-Partisan
ANDY MORIN	13	12.38%	Non-Partisan
DOUGLAS UDELL	12	11.43%	Non-Partisan
STEPHANIE C. JANTZEN	11	10.48%	Non-Partisan
NANCY L. MITCHELL	10	9.52%	Non-Partisan
KERRI M. HOWELL	10	9.52%	Non-Partisan
KEITH D. CABLE	4	3.81%	Non-Partisan
URI JOSEPH SCHORCH	4	3.81%	Non-Partisan
Intentional Undervote	8	7.62%	
Unintentional Undervote	0	0.00%	
Total	105	100%	

=====
City of Galt, Member City Council **State: CA County: Sacramento**
 Ballot Cast: 27 Skip Contest (No Vote): 0 Write-In: 0

Candidate/ Write-In	Number Voted	Percentage	Party
DARRYL CLARE	5	18.52%	Non-Partisan
JONATHAN ROTONDO	5	18.52%	Non-Partisan
MARYLOU POWERS	5	18.52%	Non-Partisan
ROB SEALEY	4	14.81%	Non-Partisan
BOB KRAUDE	3	11.11%	Non-Partisan
THOMAS J. MALSON	3	11.11%	Non-Partisan
DAN PILLSBURY	1	3.70%	Non-Partisan
RANDY D. SHELTON	1	3.70%	Non-Partisan
TERESA L. PEARSON	0	0.00%	Non-Partisan
Intentional Undervote	0	0.00%	
Unintentional Undervote	0	0.00%	
Total	27	100%	

=====
City Of Isleton, Member City Council **State: CA County: Sacramento**
 Ballot Cast: 0 Skip Contest (No Vote): 0 Write-In: 0

Candidate/ Write-In	Number Voted	Percentage	Party
DAVID AMMA	0	0%	Non-Partisan
LUIS J. DUARTE	0	0%	Non-Partisan
MICHAEL V. GOMEZ	0	0%	Non-Partisan
PAM PRATT	0	0%	Non-Partisan
PATRICIA CASSERES	0	0%	Non-Partisan

=====
City of Isleton, City Clerk **State: CA** **County: Sacramento**
 Ballot Cast: 0 Skip Contest (No Vote): 0 Write-In: 0

Candidate/ Write-In	Number Voted	Percentage	Party
LINDA S. GONZALES	0	0%	Non-Partisan

=====
City of Citrus Heights, Member City Council **State: CA** **County: Sacramento**
 Ballot Cast: 423 Skip Contest (No Vote): 50 Write-In: 0

Candidate/ Write-In	Number Voted	Percentage	Party
JAMES C. SHELBY	64	15.13%	Non-Partisan
JEANNIE BRUINS	58	13.71%	Non-Partisan
JANE S. DALY	56	13.24%	Non-Partisan
BRET C. DANIELS	53	12.53%	Non-Partisan
JAYNA KARPINSKI-COSTA	52	12.29%	Non-Partisan
JIM COOK	49	11.58%	Non-Partisan
HARRY PELLICCIONE	41	9.69%	Non-Partisan
Intentional Undervote	50	11.82%	
Unintentional Undervote	0	0.00%	
Total	423	100%	

=====
City of Elk Grove, Council Member District 2 **State: CA** **County: Sacramento**
 Ballot Cast: 140 Skip Contest (No Vote): 11 Write-In: 0

Candidate/ Write-In	Number Voted	Percentage	Party
RICK SOARES	79	56.43%	Non-Partisan
TIMOTHY DAVIS	50	35.71%	Non-Partisan
Intentional Undervote	11	7.86%	
Unintentional Undervote	0	0.00%	
Total	140	100%	

=====
City of Elk Grove, Council Member District 4 **State: CA** **County: Sacramento**
 Ballot Cast: 140 Skip Contest (No Vote): 10 Write-In: 0

Candidate/ Write-In	Number Voted	Percentage	Party
DAN BRIGGS	39	27.86%	Non-Partisan
PAT PEREZ	33	23.57%	Non-Partisan
JIM COOK	31	22.14%	Non-Partisan
RICK WEST	27	19.29%	Non-Partisan
Intentional Undervote	10	7.14%	
Unintentional Undervote	0	0.00%	
Total	140	100%	

=====
Sacramento Municipal Utility District, Director Ward 3 State: CA County: Sacramento
 Ballot Cast: 265 Skip Contest (No Vote): 31 Write-In: 0

Candidate/ Write-In	Number Voted	Percentage	Party
HOWARD POSNER	131	49.43%	Non-Partisan
JOHN W. BURTON	103	38.87%	Non-Partisan
Intentional Undervote	31	11.70%	
Unintentional Undervote	0	0.00%	
Total	265	100%	

=====
Sacramento Municipal Utility District, Director Ward 4 State: CA County: Sacramento
 Ballot Cast: 311 Skip Contest (No Vote): 29 Write-In: 0

Candidate/ Write-In	Number Voted	Percentage	Party
GENEVIEVE A. SHIROMA	162	52.09%	Non-Partisan
RICK GRIGGS	120	38.59%	Non-Partisan
Intentional Undervote	29	9.32%	
Unintentional Undervote	0	0.00%	
Total	311	100%	

=====
Sacramento Municipal Utility District, Director Ward 6 State: CA County: Sacramento
 Ballot Cast: 187 Skip Contest (No Vote): 24 Write-In: 0

Candidate/ Write-In	Number Voted	Percentage	Party
LARRY CARR	91	48.66%	Non-Partisan
GALE MORGAN	51	27.27%	Non-Partisan
TOM BRIGHT	21	11.23%	Non-Partisan
Intentional Undervote	24	12.84%	
Unintentional Undervote	0	0.00%	
Total	187	100%	

=====
Sacramento Municipal Utility District, Director Ward 7 State: CA County: Sacramento
 Ballot Cast: 162 Skip Contest (No Vote): 31 Write-In: 0

Candidate/ Write-In	Number Voted	Percentage	Party
SUZANNE PHINNEY	51	31.48%	Non-Partisan
BILL SLATON	40	24.69%	Non-Partisan
BETTY GWIAZDON	14	8.64%	Non-Partisan
PAUL MANANSALA	13	8.02%	Non-Partisan
SCHEHERAZADE MAC GREGOR	13	8.02%	Non-Partisan
Intentional Undervote	31	19.14%	
Unintentional Undervote	0	0.00%	
Total	162	100%	

=====
Elk Grove Community Services District, Director **State: CA County: Sacramento**
 Ballot Cast: 320 Skip Contest (No Vote): 43 Write-In: 0

Candidate/ Write-In	Number Voted	Percentage	Party
ELAINE WRIGHT	77	24.06%	Non-Partisan
ELLIOT MULBERG	71	22.19%	Non-Partisan
MELINDA BRAIDO	47	14.69%	Non-Partisan
GARY R. BINGHAM	25	7.81%	Non-Partisan
DAVID L. GORDON	23	7.19%	Non-Partisan
MARK A. ELLIS	20	6.25%	Non-Partisan
BRYAN B. TURNER	14	4.38%	Non-Partisan
Intentional Undervote	43	13.44%	
Unintentional Undervote	0	0.00%	
Total	320	100%	

=====
Rancho Murieta Community Services District, Director **State: CA County: Sacramento**
 Ballot Cast: 30 Skip Contest (No Vote): 7 Write-In: 0

Candidate/ Write-In	Number Voted	Percentage	Party
JOHN MERCHANT	7	23.33%	Non-Partisan
MARY BRENNAN	5	16.67%	Non-Partisan
JIM MILLER	3	10.00%	Non-Partisan
RICHARD (DICK) TAYLOR	3	10.00%	Non-Partisan
TONY PEACOCK	3	10.00%	Non-Partisan
CHARLES "CHUCK" CHRISTIAN	2	6.67%	Non-Partisan
Intentional Undervote	7	23.33%	
Unintentional Undervote	0	0.00%	
Total	30	100%	

=====
San Juan Water District, Director **State: CA County: Sacramento**
 Ballot Cast: 675 Skip Contest (No Vote): 139 Write-In: 0

Candidate/ Write-In	Number Voted	Percentage	Party
DOROTHY KILGORE	153	22.67%	Non-Partisan
EDWARD J. "TED" COSTA	151	22.37%	Non-Partisan
LYLE N. HOAG	144	21.33%	Non-Partisan
JOE PLANT	88	13.04%	Non-Partisan
Intentional Undervote	139	20.59%	
Unintentional Undervote	0	0.00%	
Total	675	100%	

=====
Florin Resource Conservation District, Director **State: CA County: Sacramento**
 Ballot Cast: 654 Skip Contest (No Vote): 156 Write-In: 0

Candidate/ Write-In	Number Voted	Percentage	Party
ANTHONY J. PEREZ	147	22.48%	Non-Partisan
DAVID BEALES	122	18.65%	Non-Partisan
SANDI RUSSELL	121	18.50%	Non-Partisan
CARL P. AMUNDSON JR.	108	16.51%	Non-Partisan
Intentional Undervote	156	23.86%	
Unintentional Undervote	0	0.00%	
Total	654	100%	

=====
Galt Fire Protection District, Director State: **CA** County: **Sacramento**
 Ballot Cast: 18 Skip Contest (No Vote): 4 Write-In: 0

Candidate/ Write-In	Number Voted	Percentage	Party
GUY V. RUTTER	6	33.33%	Non-Partisan
MICHAEL J. WEAVER	3	16.67%	Non-Partisan
ROBERT H. DEES	3	16.67%	Non-Partisan
DALE L. TEMPLETON	2	11.11%	Non-Partisan
Intentional Undervote	4	22.22%	
Unintentional Undervote	0	0.00%	
Total	18	100%	

=====
Sacramento Metropolitan Fire District, Director Division 1 State: **CA** County: **Sacramento**
 Ballot Cast: 45 Skip Contest (No Vote): 8 Write-In: 0

Candidate/ Write-In	Number Voted	Percentage	Party
H. PETER ENGELLENNER	27	60.00%	Non-Partisan
ROB J. MAC GREGOR	7	15.56%	Non-Partisan
CHARLES W. BALDOCK	3	6.67%	Non-Partisan
Intentional Undervote	8	17.77%	
Unintentional Undervote	0	0.00%	
Total	45	100%	

=====
Sacramento Metropolitan Fire District, Director Division 7 State: **CA** County: **Sacramento**
 Ballot Cast: 106 Skip Contest (No Vote): 16 Write-In: 0

Candidate/ Write-In	Number Voted	Percentage	Party
JAMES "JIM" STEWART	59	55.66%	Non-Partisan
STEPHEN R. HANSON	31	29.25%	Non-Partisan
Intentional Undervote	16	15.09%	
Unintentional Undervote	0	0.00%	
Total	106	100%	

=====
Sacramento Metropolitan Fire District, Director Division 9 State: **CA** County: **Sacramento**
 Ballot Cast: 86 Skip Contest (No Vote): 10 Write-In: 0

Candidate/ Write-In	Number Voted	Percentage	Party
GREGORY M. VALLEY	46	53.49%	Non-Partisan
BILL WIRTH	28	32.56%	Non-Partisan
JOHN G. BESSLER	2	2.33%	Non-Partisan
Intentional Undervote	10	11.62%	
Unintentional Undervote	0	0.00%	
Total	86	100%	

=====

Wilton Fire Protection District, Director - Full Term State: CA County: Sacramento
 Ballot Cast: 14 Skip Contest (No Vote): 2 Write-In: 0

Candidate/ Write-In	Number Voted	Percentage	Party
RICHARD W. MC KEE	5	35.71%	Non-Partisan
THOMAS G. "TOM" DUMAS	4	28.57%	Non-Partisan
PETER STRUFFENEGGER	3	21.43%	Non-Partisan
CHRISTINE M. MILLER	0	0.00%	Non-Partisan
ROD WOODS	0	0.00%	Non-Partisan
Intentional Undervote	2	14.29%	
Unintentional Undervote	0	0.00%	
Total	14	100%	

=====

Fair Oaks Water District, Director Division 1 State: CA County: Sacramento
 Ballot Cast: 70 Skip Contest (No Vote): 6 Write-In: 0

Candidate/ Write-In	Number Voted	Percentage	Party
BRUCE HENZ	55	78.57%	Non-Partisan
JAKE WAGNER	9	12.86%	Non-Partisan
Intentional Undervote	6	8.57%	
Unintentional Undervote	0	0.00%	
Total	70	100%	

=====

Arden Park Recreation and Park District, Director - Short Term State: CA County: Sacramento
 Ballot Cast: 7 Skip Contest (No Vote): 1 Write-In: 0

Candidate/ Write-In	Number Voted	Percentage	Party
MIKE DUVECK	6	85.71%	Non-Partisan
SALLY PERKINS	0	0.00%	Non-Partisan
Intentional Undervote	1	14.29%	
Unintentional Undervote	0	0.00%	
Total	7	100%	

=====

Cordova Recreation and Park District, Director State: CA County: Sacramento
 Ballot Cast: 393 Skip Contest (No Vote): 63 Write-In: 0

Candidate/ Write-In	Number Voted	Percentage	Party
CURT HAVEN	85	21.63%	Non-Partisan
CATHERINE (CAY) NICKERSON	67	17.05%	Non-Partisan
ERIC LUND	49	12.47%	Non-Partisan
DAN SKOGLUND	38	9.67%	Non-Partisan
PEPPER D. OCHOA	34	8.65%	Non-Partisan
MICHAEL P. PERRY	30	7.63%	Non-Partisan
BONNIE SADKOWSKI	27	6.87%	Non-Partisan
Intentional Undervote	63	16.03%	
Unintentional Undervote	0	0.00%	
Total	393	100%	

=====
Fair Oaks Recreation and Park District, Director State: CA County: Sacramento
 Ballot Cast: 142 Skip Contest (No Vote): 10 Write-In: 0

Candidate/ Write-In	Number Voted	Percentage	Party
CYNTHIA N. MARX	30	21.13%	Non-Partisan
RALPH L. CARHART	28	19.72%	Non-Partisan
ROBERT L. BROWN	24	16.90%	Non-Partisan
PATRICIA VON PETNER	20	14.08%	Non-Partisan
JAMES F. HANSEN	14	9.86%	Non-Partisan
LESTER "JIM" AMELL	11	7.75%	Non-Partisan
CHERYL F. LEFF	5	3.52%	Non-Partisan
Intentional Undervote	10	7.04%	
Unintentional Undervote	0	0.00%	
Total	142	100%	

=====
Fulton-EI Camino Recreation and Park District, Director - Short Term State: CA County: Sacramento
 Ballot Cast: 50 Skip Contest (No Vote): 7 Write-In: 0

Candidate/ Write-In	Number Voted	Percentage	Party
DEBBIE DE ANGELO	31	62.00%	Non-Partisan
BURNARD A. BRADY	12	24.00%	Non-Partisan
Intentional Undervote	7	14.00%	
Unintentional Undervote	0	0.00%	
Total	50	100%	

=====
North Highlands Recreation and Park District, Director State: CA County: Sacramento
 Ballot Cast: 30 Skip Contest (No Vote): 2 Write-In: 0

Candidate/ Write-In	Number Voted	Percentage	Party
MICHAEL L. MONK II	13	43.33%	Non-Partisan
ALAN MATRE	9	30.00%	Non-Partisan
PATRICK L. APPLEWHITE	6	20.00%	Non-Partisan
Intentional Undervote	2	6.67%	
Unintentional Undervote	0	0.00%	
Total	30	100%	

=====
Orangevale Recreation and Park District, Director State: CA County: Sacramento
 Ballot Cast: 100 Skip Contest (No Vote): 19 Write-In: 0

Candidate/ Write-In	Number Voted	Percentage	Party
MANUEL MERAZ	34	34.00%	Non-Partisan
MELISSA MANFRE	31	31.00%	Non-Partisan
CARLO TARANTOLA	16	16.00%	Non-Partisan
Intentional Undervote	19	19.00%	
Unintentional Undervote	0	0.00%	
Total	100	100%	

=====
Rio Linda-Elverta Recreation and Park District, Director State: CA County: Sacramento
 Ballot Cast: 60 Skip Contest (No Vote): 10 Write-In: 0

Candidate/ Write-In	Number Voted	Percentage	Party
ARMAND NADEAU	12	20.00%	Non-Partisan
PAULA E. PARKER	11	18.33%	Non-Partisan
CHARLEA MOORE	10	16.67%	Non-Partisan
LOREN MONROE JR.	9	15.00%	Non-Partisan
CHUCK BALDOCK	8	13.33%	Non-Partisan
Intentional Undervote	10	16.67 %	
Unintentional Undervote	0	0.00%	
Total	60	100%	

=====
Rio Linda/Elverta Community Water District, Director State: CA County: Sacramento
 Ballot Cast: 36 Skip Contest (No Vote): 7 Write-In: 0

Candidate/ Write-In	Number Voted	Percentage	Party
DOUGLAS CATER	12	33.33%	Non-Partisan
JOE GLUVERS	9	25.00%	Non-Partisan
MARY R. HARRIS	5	13.89%	Non-Partisan
CHUCK BALDOCK	2	5.56%	Non-Partisan
CATHY D. HOOD	1	2.78%	Non-Partisan
Intentional Undervote	7	19.44%	
Unintentional Undervote	0	0.00%	
Total	36	100%	

=====
Sacramento Suburban Water District, Director Division 4 State: CA County: Sacramento
 Ballot Cast: 26 Skip Contest (No Vote): 6 Write-In: 0

Candidate/ Write-In	Number Voted	Percentage	Party
WILLIAM E. PORTER	10	38.46%	Non-Partisan
MIKE SERRANO	6	23.08%	Non-Partisan
DEV BERGER	2	7.69%	Non-Partisan
ROBERT SCHAEFFER	2	7.69%	Non-Partisan
Intentional Undervote	6	23.08%	
Unintentional Undervote	0	0.00%	
Total	26	100%	

=====
Sacramento Suburban Water District, Director Division 6 State: CA County: Sacramento
 Ballot Cast: 27 Skip Contest (No Vote): 5 Write-In: 0

Candidate/ Write-In	Number Voted	Percentage	Party
BYRON M. BUCK	9	33.33%	Non-Partisan
DANIEL E. WHISMAN	9	33.33%	Non-Partisan
AARON ALLAN FERGUSON	4	14.81%	Non-Partisan
LERROY K. MUNSCH	0	0.00%	Non-Partisan
Intentional Undervote	5	18.53%	
Unintentional Undervote	0	0.00%	
Total	27	100%	

Proposed City of Rancho Cordova, Member City Council State: CA
 Ballot Cast: 300 Skip Contest (No Vote): 34 Write-In: 1

County: Sacramento

Candidate/ Write-In	Number Voted	Percentage	Party
DAVE ROBERTS	41	13.67%	Non-Partisan
KEN COOLEY	25	8.33%	Non-Partisan
PEDRO JOHN HERNANDEZ	25	8.33%	Non-Partisan
LINDA BUDGE	24	8.00%	Non-Partisan
DAVID M. SANDER	21	7.00%	Non-Partisan
ROBERT J. MC GARVEY	21	7.00%	Non-Partisan
JOHN P. EVPAK	17	5.67%	Non-Partisan
AUBRY L. STONE	13	4.33%	Non-Partisan
ROBERT E. HOTT	11	3.67%	Non-Partisan
CHARLES "CHARLIE" PARKS	9	3.00%	Non-Partisan
BECKY L. THILL	8	2.67%	Non-Partisan
JAMES R. MARTIN	8	2.67%	Non-Partisan
LOU WATSON	8	2.67%	Non-Partisan
JULIE GASBARRO	7	2.33%	Non-Partisan
JOAN ANNE FINAN	6	2.00%	Non-Partisan
PAUL R. WYGAND	6	2.00%	Non-Partisan
HARRY A. MADDEN	4	1.33%	Non-Partisan
JOSEPH THOMAS BOYD	4	1.33%	Non-Partisan
CLARENCE "CLANCY" PERRY	3	1.00%	Non-Partisan
SHAUN NEWMARCH	3	1.00%	Non-Partisan
CHRISTOPHER M. LOPEZ	1	0.33%	Non-Partisan
Alan A. CANTU (Yes)	1	0.33%	
Intentional Undervote	34	11.33%	
Unintentional Undervote	0	0.00%	
Total	300	100%	

Tally Type: Normal, Provisional
 Result Type: EARLY VOTING

Voting System: VOTE-TRAKKER™ DRE Touch-Screen

=====
 State Proposition 46 State: CA
 Housing Trust Fund

YES:	925	57.38%
NO:	630	39.08%
INTENTIONAL UNDERVOTE (Skip Contest):	57	3.54%
TOTAL:	1612	100%

Tally Type: Normal, Provisional
 Result Type: CUMULATIVE TOTALS

Voting System: Punch-card

=====
 State Proposition 46 State: CA
 Housing Trust Fund Over Votes: 272

YES:	140,887	51.14%
NO:	104,906	38.08%
Intentional + Unintentional Under Votes (Un-resolved)	29,422	10.68%
TOTAL:	275,487	100%

State Proposition 47		State: CA	
YES:	902	55.96%	
NO:	661	41.00%	
INTENTIONAL UNDERVOTE (Skip Contest):	49	3.04%	
TOTAL:	1612	100%	

State Proposition 48		State: CA	
YES:	1165	72.27%	
NO:	356	22.08%	
INTENTIONAL UNDERVOTE (Skip Contest):	91	5.65%	
TOTAL:	1612	100%	

State Proposition 49		State: CA	
YES:	890	55.21%	
NO:	679	42.12%	
INTENTIONAL UNDERVOTE (Skip Contest):	43	2.67%	
TOTAL:	1612	100%	

State Proposition 50		State: CA	
YES:	752	46.65%	
NO:	791	49.07%	
INTENTIONAL UNDERVOTE (Skip Contest):	69	4.28%	
TOTAL:	1612	100%	

State Proposition 51		State: CA	
YES:	730	45.29%	
NO:	808	50.12%	
INTENTIONAL UNDERVOTE (Skip Contest):	74	4.59%	
TOTAL:	1612	100%	

State Proposition 52		State: CA	
YES:	771	47.83%	
NO:	791	49.07%	
INTENTIONAL UNDERVOTE (Skip Contest):	50	3.10%	
TOTAL:	1612	100%	

County MEASURE G		County: Sacramento	
State: CA			
YES:	792	49.13%	
NO:	745	46.22%	
INTENTIONAL UNDERVOTE (Skip Contest):	75	4.65%	
TOTAL:	1612	100%	

County MEASURE H

State: CA County: Sacramento

YES:	908	56.33%
NO:	628	38.96%
INTENTIONAL UNDERVOTE (Skip Contest):	76	4.71%
TOTAL:	1612	100%

Sacramento City Unified School District MEASURE I

State: CA County: Sacramento

Bonds Yes:	329	67.56%
Bonds No:	137	28.13%
INTENTIONAL UNDERVOTE (Skip Contest):	21	4.31%
TOTAL:	487	100%

San Juan Unified School District MEASURE J

State: CA County: Sacramento

Bonds Yes:	351	64.40%
Bonds No:	175	32.11%
INTENTIONAL UNDERVOTE (Skip Contest):	19	3.49%
TOTAL:	545	100%

Roseville Joint Union High School District MEASURE K

State: CA County: Sacramento

Bonds Yes:	7	100%
Bonds No:	0	0%
INTENTIONAL UNDERVOTE (Skip Contest):	0	0%
TOTAL:	7	100%

Elverta Joint Elementary School District MEASURE L

State: CA County: Sacramento

Bonds Yes:	2	100%
Bonds No:	0	0%
INTENTIONAL UNDERVOTE (Skip Contest):	0	0%
TOTAL:	2	100%

Natomas Unified School District MEASURE M

State: CA County: Sacramento

Bonds Yes:	38	60.32%
Bonds No:	21	33.33%
INTENTIONAL UNDERVOTE (Skip Contest):	4	6.35%
TOTAL:	63	100%

Rio Linda Union School District MEASURE N

State: CA County: Sacramento

Bonds Yes:	42	65.63%
Bonds No:	20	31.25%
INTENTIONAL UNDERVOTE (Skip Contest):	2	3.13%
TOTAL:	64	100%

City of Elk Grove MEASURE O

State: CA County: Sacramento

YES:	95	67.86%
NO:	27	19.29%
INTENTIONAL UNDERVOTE (Skip Contest):	18	12.86%
TOTAL:	140	100%

City of Folsom MEASURE P

State: CA County: Sacramento

YES:	21	60.00%
NO:	13	37.14%
INTENTIONAL UNDERVOTE (Skip Contest):	1	2.86%
TOTAL:	35	100%

City of Galt MEASURE Q

State: CA County: Sacramento

YES:	7	77.78%
NO:	2	22.22%
INTENTIONAL UNDERVOTE (Skip Contest):	0	0%
TOTAL:	9	100%

City of Galt MEASURE R

State: CA County: Sacramento

YES:	3	33.33%
NO:	6	66.67%
INTENTIONAL UNDERVOTE (Skip Contest):	0	0%
TOTAL:	9	100%

City of Sacramento MEASURE S

State: CA County: Sacramento

YES:	325	58.77%
NO:	197	35.62%
INTENTIONAL UNDERVOTE (Skip Contest):	31	5.61%
TOTAL:	553	100%

City of Sacramento MEASURE T

State: CA County: Sacramento

YES:	263	47.56%
NO:	252	45.57%
INTENTIONAL UNDERVOTE (Skip Contest):	38	6.87%
TOTAL:	553	100%

Galt Fire Protection District MEASURE V

State: CA County: Sacramento

YES:	5	55.56%
NO:	4	44.44%
INTENTIONAL UNDERVOTE (Skip Contest):	0	0%
TOTAL:	9	100%

Proposed Incorporation of City of Rancho Cordova MEASURE W

State: CA County: Sacramento

YES:	51	85.00%
NO:	5	8.33%
INTENTIONAL UNDERVOTE (Skip Contest):	4	6.67%
TOTAL:	60	100%

A-2: AUDIT RECORDS FOR EACH VOTING UNITS

Sacramento Early Voting Oct. 15-25, 2002 VOTE-TRAKKER
EVC308

VT SN	Voters	Fleeing Voters	Spoiled Ballot	ADA Voters	Spanish	Note
VTD0200117	71	1	1	4		Market Square
VTD0200136	56	1	3			Market Square
VTD0200145	148		13	1	2	Market Square
VTD0200146	152		8			Market Square
VTD0200118	63	4	2 (1 Pro, 1 N)		3	Florin Mall
VTD0200119	59	2	3 (1 Pro, 2 N)			Florin Mall
VTD0200120	67	2 (1 Pro, 1 N)	9			Florin Mall
VTD0200121	23		3 (2 Pro, 1 N)			Florin Mall
VTD0200122	66	2	2 (1 N, 1 Test)			County Office
VTD0200123	60	1	8 (6 N, 2 Test)			County Office
VTD0200124	34		6			County Office
VTD0200129	15					Sunrise Mall
VTD0200140	100	1	6			Sunrise Mall
VTD0200142	129	3	6 (1 Pro, 5 N)			Sunrise Mall
VTD0200144	124	1	6			Sunrise Mall
VTD0200130	52		1		1	Elk Grove City Hall
VTD0200135	52		6			Elk Grove City Hall
VTD0200141	24		3			Elk Grove City Hall
VTD0200133	49	1	1			SOS
VTD0200134	6		0	4		SOS
VTD0200137	60		7 (1 Pro, 6 N)		3	SOS
VTD0200138	114	1	1		1	SOS (Recount VT)
VTD0200126	88 (Pro)					Provisional VT
VTD0200127	12 (Pro)					Provisional VT

ATTACHMENT B

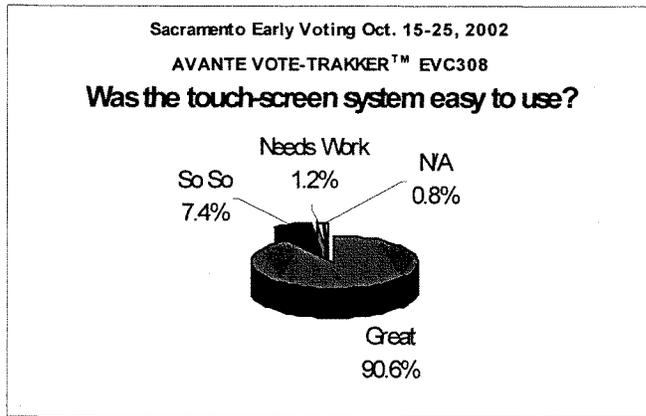
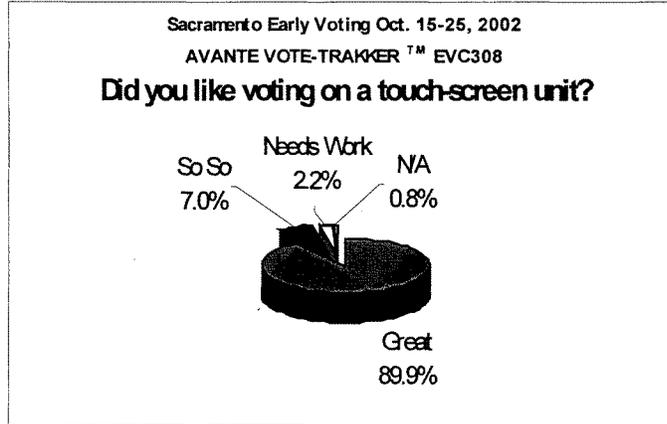
REPORTS ON THE RESULTS OF THE
SURVEYS OF VOTERS AND POLL
WORKERS

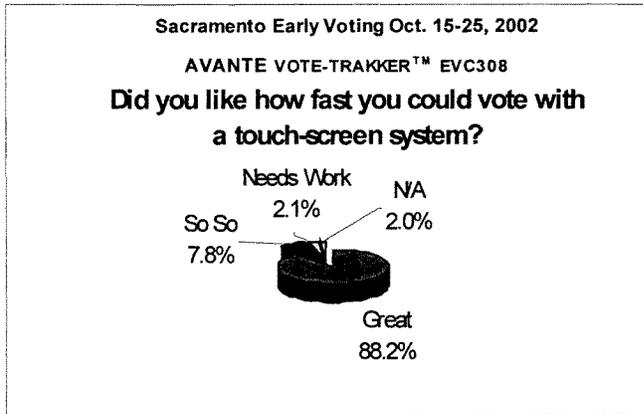
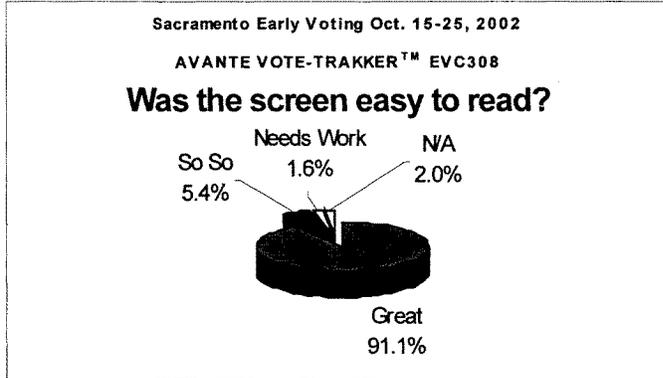
B-1: SUMMARY OF THE RATING MADE BY VOTERS

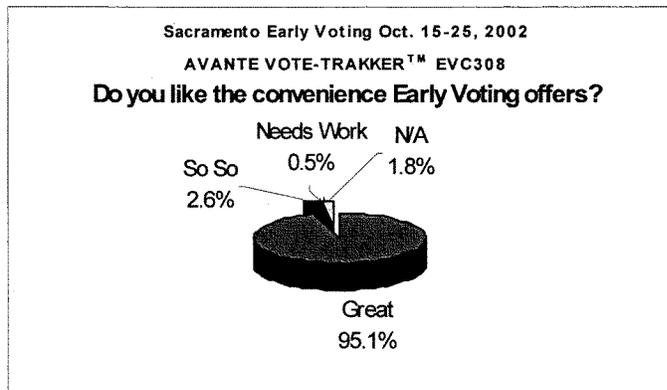
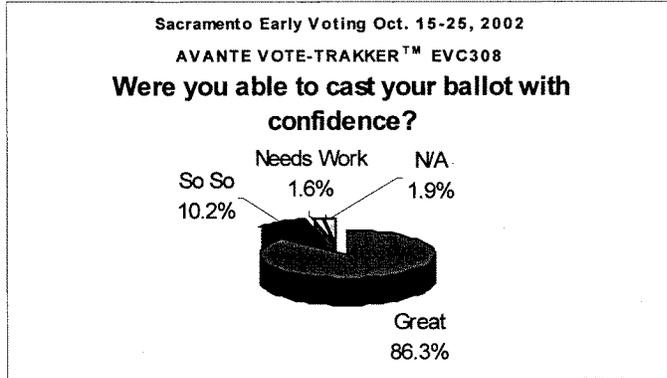
Total no. of voters for early voting	1624
Total no. of questionnaire received	1208
%	74.38%

Question

1	Did you like voting on a touch-screen unit?			
	Great	So So	Needs Work	N/A
	89.9%	7.0%	2.2%	0.8%
	1086	85	27	10
2	Was the touch-screen system easy to use?			
	Great	So So	Needs Work	N/A
	90.6%	7.4%	1.2%	0.8%
	1094	89	15	10
3	Was the screen easy to read?			
	Great	So So	Needs Work	N/A
	91.1%	5.4%	1.6%	2.0%
	1100	65	19	24
4	Did you like how fast you could vote with a touch-screen system?			
	Great	So So	Needs Work	N/A
	88.2%	7.8%	2.1%	2.0%
	1065	94	25	24
5	Were you able to cast your ballot with confidence?			
	Great	So So	Needs Work	N/A
	86.3%	10.2%	1.6%	1.9%
	1043	123	19	23
6	Do you like the convenience Early Voting offers?			
	Great	So So	Needs Work	N/A
	95.1%	2.6%	0.5%	1.8%
	1149	31	6	22







B-2: GROUPING OF WRITTEN COMMENTS FROM VOTERS

The following points should be noted from these comments and suggestions:

1. The comments and suggestions are made in addition to the rating.
2. We have grouped the comments using our own judgment.
 - ◆ **In the accompanying letter to Mr. Jennings, we explain the modifications that will be made to the VOTE-TRAKKER™ EVC 308 to address some of the comments received, including adjustments to the prompt and highlighting features.**

PRAISES ON THE USE OF VOTE-TRAKKER™ SYSTEM

569 This was fast, fun, +easy!
551 Every thing was great thank you.
553 I hope this is installed all over the United States
545 This system is very user friendly + easy. Should been done this way all along.
561 Great improve program.
572 With this system there appear to be less need for absentee ballots and their cost.
565 This should be the norm for all California
582 Great system!!! Convenience is spectacular.
583 I like being able to vote early and I have much more confidant in the accuracy on the vote
587 This is so much easier than trying to punch hole in a piece of paper
514 It is great to be voting like this.
511 MORE OF THESE EVERYWHERE!
520 Could use a little more difficeacition on the tittle of props+ positions. Great design overall! Thank you.
672 Screens moved very fast but I really liked it
665 This is great!!! Explanation was very good, process was very easy & I love that it fit my schedule.
666 Great system and idea of voting touch screen! Loved to be able to vote early due to schedule conflict on Election Day and absentee voter registration accidentally thrown out. Extremely convenient to do right in the mall
524 Blind.voter. Employees/ volunteers were very helpful
528 great time saver
532 Fantastic
534 GREAT
650 Good job
652 Fun
654 Great start on new system Thanks
655 Great stuff we appreciate your help
659 Great easy fast & redundant
660 Excellent technology
647 Excellent system sends it to Florida good training Thank you
648 I like it!!!
642 should be implemented statewide
628 I work for SOS elections & I loved it
615 I actually vote faster with the punch method but I loved to be able to vote at my convenience
616 This is great! We need these everywhere
618 Keep this up & expand!
599 this is a great idea makes it easier to read + vote
600 great system
602 get this online!!! It would be great. Master card can be used online. Get an imprisoned hacker to develop an encrypted ID system to protect voter ID and go with it thanks
590 Excellent system that will become even easier to use after a few election cycles.
588 Very easy to use.
589 I think instant runoff voting is a needed reform and that computerized voting facilitates this computerized voting is good
811 I like it very much.
812 I liked working with this new style
808 This is terrific had a very good demonstration of how the machine works. Volunteers helpful + friendly + efficient. I didn't have to wait + wait (like before) to have the volunteer confirm my status to vote.
804 Great
805 Long overdue early voting is a must!!
681 yeah! Thanks.
706 Thanks for moving the voting experience into the 21st century!! And may god bless all of you & your.
Mike de Santos
702 If you can read, you can vote. Please bring your ballot. Save time. Learn to read.
693 excellent instructions and easy to use voting system. This should be used everywhere.

694 would like to use it on Election Day. I wish there were a way of speed thew voice. Would like the four keys closer, but was able to use second hand. During voting for some officers/ propositions. Instruction was part of ballot title. Repeated instruction.

700 very efficient.

683 this worked great. I really enjoyed voting this way. So much better than punch cards.

684 I liked It!! Very convenient

686 excellent

687 easy, fast

688 excellent voting system appreciates the convenience of being able to vote early. Great way to review ballot at the end with the printed receipt.

680 definitely better then punch cards fast easy. May encourage younger voters because it seems modern.

677 very pleased Warren Chasman. Voter since 1958 blind. Phone # 916-488-5125

79 I would confirm on the pop-up screen after touching who I voted for instead of "next". Great!

62 Let's do it! :)

63 All good.

59 Wonderful need more!!

41 Very good experience. Suggest-selections should "Hilite" when you touch before "next selection"

22 Excellent!

29 Thanks for making it wheelchair accessible!

15 1. It would be nice for a tray/table/ledge to put voting book on? 2. Excellent screen with some privacy 3. Loved viewing list choices to double check with my book 4. Maybe consider adding #'s like matching with book?? But screen was great for "old" eye

16 Fantastic !!

17 Very fast and efficient, I did like the paper receipt to be able to view how I had voted. There was a sense of security.

19 About time. Help other states - like Florida

14 This is an amazing system that will surly bring more people to voice their votes.

7 Absolutely easy

210 very good like voting on a touch-screen unit.

207 It was great and the training very helpful.

162 This was wonderful, I would use this every year if available!

163 I liked the confirmation/summary screen prior to submitting the ballot.

168 Excellent idea !!

181 Screen very easy to read. Yes, like how fast I could vote with a touch-screen system

187 Awesome

189 Pretty good deal going should do this every where. Needs to be a little bigger for reading. Thanks.

121 Enjoyed - quick easy to read- lots of help. Thanks.

122 Easy to vote like this. It would be nice. If the computer offered info on candidates.

124 loved it!

107 I really liked the touch screen voting system I hope it will soon be permanent in Sacramento.

106 The experience was fun, simple and comfortable. The poll workers were nice and friendly very helpful.

102 I think the whole voting system should use this early voting system.

127 Very convenient, easy to use and operate. Highly recommended!

101 It was the best ever!

968 Great improvement- Let's do it!

970 Its time has come!

963 This is so much easier than the old punch cards! Loved it.

942 What a pity that it has not been in use over all the years.

957 Great!

940 Good system!

929 An idea whose time is overdue! Kudos to user-friendly staff (Both human & electronic)!

928 Great!

925 Great systems. Wish we were using them on Nov. 5th.

877 Great idea - let's make this available at all of the malls for weeks and week before each election.

878 The voting procedure was simple + quick. Great idea!

879 Great program. Great helpers.

880 Great system!
873 Very quick + explanatory. I especially like the brief description of the propositions & measures.
865 I loved it so so much easier for me
854 This system works + is time saving. Thanks.
845 Good job!
847 I'd like to make sure that my vote is secure. But otherwise, I liked the touchscreen voting.
849 Works great!
841 Thanks-Great!
842 Loved it! It may have been easier/faster if numbers had been included (similar to the booklet we received.)
by the names.
838 I have been praying for this. No more hanging chads!
833 It is new but it is easy to learn.
493 A fabulous system - love voting before Nov.5th!
488 Great idea!
470 This is much better than the old way.
474 Make it nationwide!
455 Well this was my first time doing this.
457 Buy
458 The use of the machine was great. Was explained real good before you started.
448 Everything fits after use.
440 Great system - hope there are no bugs in it!
442 It's great for people who are disabled. Thank you for the experience.
435 Hope we have this method soon.
411 It's nice new machine for voting, but for the first time voter it is still need some work. I think the voter
should have a copy of the result and read it to make sure if the candidate is the right one.
413 Super!
414 Excellent and Quick and Well explained.
419 Good.
422 Very easy!
407 Let's see Florida mess this up.
402 Excellent for Sacramento!
391 This is a fabulous way to vote!
389 This is something that's really needed. I love it.
295 Good idea.
293 Needs a stand connected to PC to hold ballot. Also should have number option, would be faster. But overall
it was great!
292 This seems to be a way to facilitate voting and that will increase participation, hopefully.
290 Very thorough and convenient.
287 I think this is the best thing that was done for this no mistakes and you can review before you make a final
cast of vote.
283 about time
284 Should alleviate long lines!
266 We needed these touch screens last year! Thank you for the convenience and for saving a whole lot of
time!
262 Blind voter: This is the first time to vote a private ballot. 1. The vocal instruction does not clearly state
that the minus key would not re-read the current candidate. 2. Offer the choice to speed up the reading. 3.
System hangs once. Keyboard does
258 #1. Voting touch screen was great- didn't like however, the time it took to surrender AV & filling out
documents/cards. Would have been helpful if given tips, such as : electronic eye, etc. Although Demo was
available, it is cumbersome to finish out a demo
249 Painless. We need to purchase these units. The crowd was cheering that finally Sac. Get a voting sys that
work well for all of Sac.
255 This is the way to go!
256 Way to go!
238 I found the summary of my votes to be very useful and far less confusing than the old paper ballots.
232 This is a HUGE improvement over the old Punch System.

- 233 Very good experience.
- 225 This was the best!!!
- 212 Very easy to use and understand.
- 218 All great
- 1296 I think this is a great idea with computer system like they are now. It is about time Calif. reached the 20th century.
- 1297 Best inventions!!!
- 1298 No hanging chads--great convenience
- 1279 Very user-friendly!
- 1283 Obviously-- I think it is great!!
- 1275 I look forward to this being available at regular polling locations.
- 1276 Those was easy.
- 1272 Simple Simple Simple! Any one can do this!
- 1267 Excellent way of voting. Easier to count accurately and fast.
- 1263 Great idea. I would even be better if could vote over internet.
- 1260 Thank you!
- 1251 Very easy!
- 1249 Glad I was able to try it out.
- 1246 Great!
- 1244 Personally, it did not make that much difference over punch card. But it will obviously help in tabulation.
- 1242 Able to review and change vote if want to . Great.
- 1222 Electronic voting is the way to go.
- 1216 Great system!
- 1204 It was beneficial to be able to review my choices before casting the ballot. Great system, also gives people options when voting early.
- 1199 Very nice-- but would like ballot "Tab" like punch system let us keep.
- 1201 Good Luck!
- 1186 Great improvement.
- 1187 Much much better!
- 1184 Very smooth system. I did have to concentrate a little on the propositions.
- 1165 Why the effort to make voting into rocket science? A piece of paper with names and "Yes" & "No" works just fine. But this system is a lot more sensible than the present incomprehensible system.
- 1166 Awesome- the only way to vote!
- 1167 Very convenient!
- 1164 I hope we get the new voting system less than the 2 years. I have confidence in Cray Davis!
- 1163 Suggest to implement system. Staff was very helpful and friendly.
- 1157 Very easy to use!
- 1147 This will eliminate the problem of hanging chads.
- 1143 Great touch-screen system. Very easy to use and understand. Like the receipt at the end. Confident in recounts and ability to use in the event of a lawsuit. A keeper!
- 1130 Highly recommend this method of voting.
- 1128 Great-as a trial time shall tell of any possible flaws
- 1132 The punch cards stink & always did - get rid of them.
- 1133 I hope everybody in voting by computer, such as this would like the system. The system is fool proof.
- 1136 I think the software could be more user friendly. Overall, very nice system. But could be confusing be too many prompts, could be more detailed, ongoing, as to who you are voting for.
- 1138 This was easy. I loved the early election voting opportunity.
- 1139 They should install this system everywhere to increase voter turnout and make voting easier and more convenient for everyone (especially in Florida!)
- 1140 Everything was fast easy, great. Two suggestions: make an immediate "Correction" button available on screen (unless I missed it) and please make the receipt font size larger if possible.
- 1150 Love it!
- 1100 A big improvement and very convenient.
- 1101 This is a great way to vote!
- 1102 I'm pleased with the experience both the touch-screen voting and the opportunity to vote early,

1103 I have confidence in the touch-screen unit. My "Haha" means lack of confidence in my voting choices.
Sorry about the joke.

1104 Quick and easy to use. I liked this a lot.

1099 very awesome to be able to come in early and vote so quickly.

1093 Good show.

1086 Excellent, this is the best method for older voters. Thanks.

1087 a much quicker system.

1088 Great experience!

1089 Terrific!

1082 Loved the experience!

1090 Too tall, had to bend. Overall great experience. Would definitely do this again.

1077 It's better than alternate sites and it kills time faster. Great!

1059 It was a wonderful experience. Very easy. It also works out great since I wasn't sure if I could vote on the 5th due to going on a trip.

1052 Love it!!!

1017 This system seems to work great, and is much easier!

1020 Big improvement!!

1004 Love it!

1038 On some issues I found the machine tried to hurry me along and I was familiar with issues.

1032 Convenience in voting will certainly result in a higher turnout. Bravo!

382 Super!

362 Touch screen voting is wonderful!

352 Great idea

306 Every thing is great. We should have done this years ago.

1045 Printing on receipt was too small to read. Otherwise the system was very easy to use.

312 Early voting to us a real blessing. System seems easy enough for anyone to use.

1005 Touch screen is the best way to go. I will also be watching (after the election) how successful the tabulation are. I am expecting it to be much quicker.

313 Very good!

314 Should be at every poll.

315 Very fast.

320 This was enjoyable to poll here and was extremely easy to vote this way.!

321 Very good. I will use it again.

329 Excellent

374 It is about time for electric voting booths . Hip, hip, hooray!

334 Great!!

336 Loved it.

339 I think it a good system.

347 The touch screen was very easy to read; However, my suggestion is that the "make your selection" text that flash on the screen is; aced away from the text the voter is reading.

356 Great!

360 Do hope this voting unit be used in all voting places.

366 I felt a little rushed, probably because I'm not used to computer, otherwise I felt it's much better than the old method. Printout?? Could be better on the screen.

368 I liked the pre-final review screen + 2 touch-confirm. It would be a bit easier to use if the numbers by the selections on the sample ballot were included on the touch screen selections.

373 I think it is much easier if #'s are next to the choices as this is how the sample ballots are printed.

384 I hope it works. It looks like a great improvement!

1033 I recommend the conversion to electronic voting.

1034 Great.

1025 We need early voting with these electronic machines!

SUGGESTIONS & COMPLAINTS OF "PROMPTING"

575 If you are moving slow reading it tells you to hurry which can throw off the thought process.
571 When the flashing message appears I can not vote until it goes away.
564 the prompting to make a decision tented to make me want to believe there wasn't a place for the voter concentrate so it was different to coordinate the voting screen and looking at the proposition.
566 Need to be a speed reader.
525 The prompter to vote pls. Make your selection I did not like.
516 The "make your selection" screen was to quick to appear.
504 Did'nt like how it started flashing a message while I was checking how I wanted to vote.
536 A little confusing I've used other machines I liked better such as Diebold.
633 This was great a wonderful option. I'm going out of town in 36hrs Never received my sample ballot. The only suggestion for the machine is to give more time before the " make selection " prompt hurry up Thanks!
651 when done and reviewing selections it flashes make selection this was a little disconcerting
632 I think it comes up with "please cast vote" too fast otherwise it was good.
621 don't have the please make a choice" prompt come up so quickly when there are more then 6 choices it's hard to read them all.
625 That 'please make your selection" message is irritating especially when your trying to read measure.
635 The message that reminds the voter to please make your selections comes on too fast before you can read the screen.
636 too quick on the please vote flash
591 Allow more time to review the screen contents before the reminder prompt starts flashing [makes it harder to read have to time your reading between the flashes
822 after voting and while removing my selection, I did not like the "make Selection" message that kept flashing on the screen. After final cast ballot, the typed ballot was restarted before I could verify everything I would prefer internet voting, with simil
813 The screen don't allow enough time for reading propositions would not let me see the additional info.
817 please extend the time especially in reading measures some of us read slower than other. Thank You.
806 a little too fast.
800 While reviewing my ballot the "please make your selection" note came on too soon and was distracting.
713 I would have liked to persue over the choices half a second more before the "Make a selection" logo appeared. Also the plastic guards over the print out could be a little stronger on the attachment to the machine I knock my down accidentally. This was a de
seems very easy and fast could give a little more time to cast vote felt a little rushed.
703 Give me more time before the "make selection" pops up on the screen. I would recommend 1 minute.
696 needs to be slower for measures.
689 give people more time to read the issue prior to flashing "please cast your vote" banner.
679 amount of time on propositions & blinking picture.
86 The reminder to "please vote" kept popping up because I was still reading. I found that annoying & it distracted me, causing me to go even slower. I wish I could see who I voted for before it moved to the next screen, instead of having to go back & look.
76 Screen should not flash " please make selection".
72 Think there should be maybe 60 more seconds per vote to quite the person an oppportunity to read and think about the selections. Otherwise, ok I was pleased.
65 wanted more time to consider my vote-prompt make me anxious
61 I don't like how it rushes you to vote you should have to rush it might make voters like me. Other than that it's great and I really enjoyed it.
53 There was no way to tell that my choice was selected until the very end. When my selection was made, the screen flashed a message, then moved to the next screen. I was not certain that my choice was selected until I was able to review the final screen.
52 I don't like the screen prompt to "Hurry you"! I want to be able to vote at my own pace without this distraction. I feel older people may become frustrated at this prompt and select the wrong box and have to review votes. This uses more time. Get rides o
51 Must be prepared to vote in advance

- 36 I had made my selections but was still reviewing them. I had the voter information guide in my hand and I apparently accidentally touched the screen twice with the center of the open guide because it took my choices and spit out the receipt. I was done b
- 35 Flashing reminder to vote was a bit annoying.
- 30 The "please make your selection" flashing message was a bit annoying as I tried to read longer propositions. Maybe it could come on 30 seconds later. Thanks. :)
- 21 1. The "hurry up" feature is a bad idea. 2. Again (in the interest of speed), there's not even a second delay to see who was voted for.. Until its all over 3. Wasn't faster for me (but I'm fast in the booth). 4. Didn't have my sample ballot #s/names no
- 13 Nice surprise to be able to vote today, early . If the system would allow the user a bid more time before prompting to make a selection, the experience would be even nicer.
- 12 I was annoyed with the constant reminder to make a choice so quickly - otherwise, this was a great experience !! :)
- 9 Please remove the blinking selection warning.
- 2 I do not like the flashing message covering the text I'm trying to read
- 4 The only change I would like is to allow more reading time before the banner reminding the voter to "make your selection" appears. It made me a bit anxious to have it flashing at me while I was trying to read, and I imagine it would be worse for someone no
- 1 Machine rushed me. Unsure at first if vote registered (then noticed the little line)
- 199 Screen may be difficult for slow readers
- 180 Don't like the (please make your selection)
- 164 Selection reminder came up just a little too soon when I didn't make a selection right away. I felt a little rushed.
- 158 The "please make a selection" box that kept flashing while I was reviewing my ballot was annoying. Also, we used to get stubs / a receipt after voting. It would be nice to get a receipt after touch screen voting.
- 152 Wait longer before "make your selection" alarm flashes.
- 146 Flashes " make your selection too much! Makes me nervous! Thought I needed to touch something or the screen would go blank!, Like the convenience of Early Voting offers !!!
- 992 Needs to have a longer time to read screen.
- 978 Machine does not allow enough time to thoroughly read written proposals.
- 977 Voting would be faster if issues were also keyed to numbers on sample ballot.
- 962 Use the numbers like the old sheet. Selection should light up or flash after touching
- 943 I do like it but I think I'm just used to having the #s with the ballot
- 939 It would be good if the numbers to the left of the names would also be on the screen.
- 933 Numbers on sample ballot not on touch screen.
- 923 Proposition number on screen need to be much bigger. I.e. like the text!!
- 920 The system did not give you enough time to make a selection. When reviewing my ballot it kept flashing "Make a selection" in the middle of the screen. More time is needed!
- 921 Screen asked you to vote or "Make your selection" a little too quickly- add a few more seconds.
- 915 "Make Selection" annoying- not enough time to review. Numbers instead of names?!
- 907 #4. May be a little too fast.
- 860 Sheet of total voting retracted too fast to completely read it. Instruction is needed.
- 892 Need more time button
- 896 Some questions were too fast.
- 876 The prompt is way too quick (the one asking if the voter has made a selection yet). Very aggravating!
- 871 The only thing I didn't like was the naggy "make selection" reminder that blocked part of the screen + seemed to be trying to rush me along.
- 862 Rushes you a little.
- 864 Needs a little more time before starts prompting for "Next"839 The cue to please cast a vote when I paused to consider a particular set of candidates came on too quickly. It should wait a little longer.
- 837 Flashing comment stating direction to make a selection was distracting. As this was an unexpected encounter, I did not have my booklet with me. Therefore, I did not have needed information about the candidates.
- 498 Stop, or wait longer to warn people to "Cast you ballot" or to hurry up and select. It take some time to read everything, the reminder made me feel rushed. Wait longer to warn the voter. Give them time for read everything if they want.

- 500 I did not like the flashing- " please make your selection" why not have access to more info- like voter handbook I did not like the paper that come out at end - hard to read.
- 492 Did not like the "please make your selection" notice on the screen. It made me feel rushed.
- 490 I think the reminder on screen pressures voter unnecessarily to move on and increases errors.
- 487 Need to allow a little more time to make choice prior to message appearing to make a choice. May cause panic in some users/voters.
- 388 Please do the early voting system!!!
- 300 Great option! I really needed the convenience.
- 297 This facility should be open up until and through Nov. 5--8:00 PM. This should not close on Oct. 25, 2002!!!
- 410 Moves too fast to read or made decisions
- 288 The machine rushed me with messages "Please make your selection". That was annoying, get rid of it. Also, the selections need to be numbered as they are in the sample ballot. I also didn't like the message screen that came up after I selected. "Next Contest
- 275 It should give more time for reading, new voters don't read English fast, Adult ESL special.
- 282 The "please cast your vote" seemed to rush me.
- 263 The only thing I did not like because it rushes you through the voting process!
- 257 Please make selection pops up too soon and too often.
- 247 Please take away the "make selection" screen that pops up too quickly.
- 248 Flashing prompt - please cast your vote was annoying.
- 242 Paper read out too sensitive. I couldn't read it that close and it disappeared before I read 4 lines.
- 237 The "Next Selection" text is left-justified and appears to highlight one of the selections. Should be centered.
- 235 1) Don't rush voter!!! Get rid of the flashing prompt! 2) Moving away from machine caused problems. Fix or warn. 3) I intended to review choices after I finished- but was not able to do so.
- 1271 You have to review printout quickly.
- 1295 Need more time to read the measures. The bar that pops up to make your selection was way too fast.
- 1299 #4 Flashing directions to choose did not leave time to "think" about your choice.
- 1285 Machine froze in middle of voting- had to void and start over. Measure and candidates don't stay on screen long enough.
- 1247 need more time to read ballot before voting
- 1250 The machine seemed to try to rush you to conclude. I don't think you need to flash a reminder. If so it should be slower.
- 1221 Blinking cast vote was annoying and covered a candidate's name. A "Back" button would be nice instead of at the end.
- 1214 For the city school board category, I only casted 2 votes and the screen message continued flashing for me to make the final selection. I only wished to cast 2 votes and then pressed "skip ballot". For a while, the screen message was giving me the impression
- 1196 Did not like the "please make a selection". Could be placed elsewhere!
- 1212 Voters definitely need to be prepared and educated on the issue before using the machines are so quick.
- 1160 The tag "Vote Now" keeps popping up once the wording in the measures making them hard to read.
- 1161 The only problem was the screen kept prompting me to make a selection while I was trying to read the initiatives. Slow down the selection so you can read the screen.
- 1170 I did not like how if I took a little too long to decide . The "please make a selection" prompt came too quickly. Also I would prefer to get a printout of how I voted.
- 1171 #4. Felt a little rushed at times.
- 1185 Move the flashing cast vote now/make selection, etc. In the middle of the screen while I am reading.
- 1141 For the propositions, a little more lag time to read text before the prompt appears I wasn't sure what to do when the paper came out -maybe more instruction on the screen?
- 1126 The computer did not give enough time to read the entire selection before asking you to move along.
- 1129 Screen gets to impatient, need more time to read candidates.
- 1131 Flashing reminder is disconcerting- needs to be adjusted for frequency.
- 1136 I think the software could be more user friendly. Overall, very nice system. But could be confusing be too many prompts, could be more detailed, ongoing, as to who you are voting for.
- 1140 Everything was fast easy, great. Two suggestions: make an immediate "Correction" button available on screen (unless I missed it) and please make the receipt font size larger if possible.

- 1137 I did not like the flashing "Cast your ballot" or "Make your selection" that came up while was reading. It was annoying, came up too soon, + blocked the wording. Otherwise it was quick and easy.
- 1156 Longer decision time before prompt to place vote. More candidate information.
- 1094 The prompt to vote is a little too quick on some of the ballot measures that take longer to read.
- 1098 Needed more on the propositions- but it was convenient, quick and easy. Maybe it will encourage more people to vote.
- 1105 A major problem I had was that after a few seconds a phrase would start blinking on the screen which read "Please make a choice" or something like that. I found it very annoying, and felt as though I were being rushed. Another problem I found was the glare
- 1106 Dislike the flashing info message to cast the vote within a period (short) of time. I did not have my prepared ballot with me to refer to at this time.
- 1112 Didn't like the "Make your selection" that kept flashing. It made me nervous for I just wanted to re-read the propositions one last time before I made my final choice.
- 1113 Prompt was annoying.
- 1085 I resented that they printed "Hurry Up" -- It made me feel pressured unnecessarily.
- 1081 While reading the screen, after about 1 min a "please make your selection" appears over the text I am reading. It slowed down the process.
- 1078 Needed more time to read info on some of the specific bills, but otherwise a great system!
- 1074 A few more seconds to make selection, before it starts blinking. Move blinking message out of the way so we can read what's on the screen.
- 1048 Might be a little too fast with the "Cast your choice". People need time to think without being pressured.
- 1030 All in all the experience was great. The only critique I have is that there wasn't enough time allowed to read over the selections before the "Please make a selection" bar pops up and I never saw a scroll bar.
- 1053 not enough time to read initiatives.
- 1027 The "Make your selection" prompt interrupted some of the reading. But, I think this is a good system. Thank you.
- 1022 It prompted for my choice a little too quickly..
- 1035 Need to remove the sign on middle of screen. Annoying. It was fast. Learning time for public will be a problem unless done in mass or through media.
- 1012 The system hurried me in my voting maybe a "wait button" to add 30 seconds.
- 346 Touch screen rushes you
- 347 The touch screen was very easy to read; However, my suggestion is that the "make your selection" text that flash on the screen is; aced away from the text the voter is reading.
- 350 Machine does not allow you enough time to review your ballot.
- 351 Sacramento City unified district. I only was able to vote for three people before the next change came up.
- 1114 There appears to be a time constraint in the voting process. Please remove pop-up windows that force me to move quickly.
- 1031 Give voter more time to read. The choice picked should be highlighted. Can't really review the paper enough before it pulls it back it.
- 1009 Flashes over wording, and is annoying.
- 354 The screen rushes you and the pop bothersome, too fast and makes it hard to stay focused on what you're reading. Pop up should be a little more paced.
- 366 I felt a little rushed, probably because I'm not used to computer, otherwise I felt it's much better than the old method. Printout?? Could be better on the screen.
- 1007 When attempting to read screen messages, say propositions, the center of screen turned white & flashed & made it difficult to read & nerve wracking when kept flashing "Vote!"
- 1008 Method of reviewing ballot was not clear. Message for next contest covered up names. Move over a bit to right and wait a few seconds before switching screens.
- 1023 The blinking "Please cast your vote" icon was very distracting and made it extremely difficult to read the informational paragraphs on different ballot measures. Other than that, this was wonderful. The staff was very helpful and made the whole process ver
- 1039 I didn't like the blinking sign asking me to hurry with my vote. It interferes when I try to read the screen.

ON PRINTED PAPER RECORDS/RECEIPTS/BALLOTS

- 670 I the paper copy of my ballot I feel confident in the ability to keep these elections honest w/computers.
- 518 Why keep results if you can't keep them?
- 664 Computer sucks paper back to quickly when I bend over to look at it
- 506 I prefer the touch screen system that show you your completed ballot and offer the chance to change selections before casting the ballot. The paper receipt, even with this limited ballot moved "too fast" and the ballot was already cast.
- 656 The details section is great addition. Good to see that hard copies are kept as well. Questions where does the write card go?
- 578 The paper verification slip that come out after completing to vote was inside a plastic cover that made it hard to see and it was down too low and was quickly pulled back in to the machine this needs work.
- 638 No hard record of my vote
- 631 Need the ability to review final paper ballot (and have an opportunity to "correct" in errors in voting) at more leisurely pace
- 824 I would like some kind of receipt to show that I voted-besides a sticker. Maybe the final ballot could be higher so people could see them better.
- 661 couldn't review final ballot didn't work for me!
- 179 It would be nice to be able to take home a "receipt" of your choices. It would be nice to have immediate confirmation of your choice rather than only at the end.
- 171 Needs to signal your choice at the time you're making it (highlight ?) to increase certainty.
- 980 Difficult to read receipt with bifocals. If typing of write-in isn't done quickly enough the voting stops. Alphabet was scrambled to work with people who type - would have been easier for me if had been in alphabetical order.
- 961 I would like to be able to receive a printed copy of my vote.
- 994 #5. I would suggest increasing the size of the print on the printed ballot. It was difficult to read the
- 856 Great to have receipt to double check the vote!
- 852 Very helpful great early voting. Receipt response easy to read and fast.
- 851 Would like to have had more time to review the receipt.
- 843 The printout is too small + too low to read with any accuracy.
- 835 I like the receipts because it gives you the confidence that your vote was cast as opposed to relying on computers which malfunction from time to time.
- 829 The printout was a little difficult to read. The time allotted to read candidate and/or measures could be a little longer before the "beeping" begins.
- 824 I would like some kind of receipt to show that I voted- besides a sticker. Maybe the final ballot could be higher so people could see them better.
- 469 I like paper receipt.
- 219 I love to be able to verify what I voted for with the slip. Excellent!
- 1219 I would like a receipt or stub indicating I voted, where, when etc. I would have liked literature/info on ballot items available to me. Knowing that early voting is available, I could better prepare myself.
- 1154 We need to be able to change our votes if needed. Get the system going. We need to have a receipt to keep.
- 1127 Suggest some form of receipt should be available to indicate the voter actually voted.
- 1134 the print out receipt is too small. Receipt is OK to have.
- 1149 I like the large type- easy to read. I hesitated to move back from the printed receipt because I didn't want anyone to see my vote. It is a good check. How do you clean the screens? Sanitation concern.
- 1021 Touch screen sensitivity may be need to be increased. Also additional information on candidates, position statements, and analysis should be included as well.
- 342 I'm impressed with the paper ballot also.
- 348 Found it great - liked being able to read propositions easy to read and follow directions. Please buy.
- 366 I felt a little rushed, probably because I'm not used to computer, otherwise I felt it's much better than the old method. Printout?? Could be better on the screen.
- 1024 Is it possible to have a running tally along one side of the screen. I would like to have more time to review the paper receipt.
- 1041 What does the voter get after voting? Now they get the "Stub". With the new system, they get nothing. How about a simple brochure (8 1/2 X 11-0 folded-4 sides) that explains the process with "Q&A's" from real voters. Jim Keating, Coordinator. The she

- 1045 Printing on receipt was too small to read. Otherwise the system was very easy to use.
- 1058 maybe a paper receipt that you've voted?
- 1092 Larger print out for checking

SUGGESTION TO ADD NUMBER SIMILAR TO PUNCH-CARD BALLOTS

- 513 The number would have been easier to recognize who you're voting for.
- 637 It would help to have numbers next to the candidates as it appears in the sample ballot book allow more time before the flashing make choice begins
- 531 Sample official ballot has numbers that correspond with names(as used on punch cards]. It would be helpful to have these numbers on the touch screen as well.608 the number of each selection s shown on the "Sample Ballot" should on the screen
- 596 please add a link to read about measure or candidate during voting
- 595 Would like the #'s that appear in sample ballot
- 801 proposition numbers should be bore clear.
- 80 Not fast, love it Early voting. Need #'s at side - some people don't read well and then you can correlate.
- 56 Please make sure the number on ballot matches what we receive.
- 40 For now, the actual # we have on the booklet could be prominent and speed things up even more.
- 34 1. Should have had the numbers next to it like the sample ballot. 2. For the justices, it didn't have their names on it. 3. It wasn't as fast because it was difficult to verify what I entered. Need to read printout also. 4. Absolutely great for early
- 20 Does not show balloting by numbers as sample ballot sent to home.
- 204 I brought my cover from my ballot with all the numbers marked and didn't realize I needed the whole ballot with the names, etc. on it. This should somehow be conveyed to voters so they don't do as I did and not have everything before them. I had to skip
- 198 1. Would like partial scrolling in review. 2. Punch-card no. on each item (ref #). 3. Way to skip entire race where multiple items are to be selected.
- 194 Would like to have punch position numbers on screen to coordinate with ballot sample provided with voter hand book.
- 129 It would be very helpful to have numbered screens and a back screen button. A flashing messages came up while I was reading. That was a distraction.
- 128 I miss the numbers in front of candidates names. However, if a person can read, the correct name will be punched.
- 126 If I lingered too long, if I paused too long on 1 item, machine wanted me to vote ASAP.
- 90 I thought the last system was better. I could pre-mark my ballot and could check the punch with my pre-marked ballot. This way I have to go through each page of my sample ballot.
- 105 I would like to see the numbers added to the screen.
- 123 Numbers would make it easier to mark ballot
- 991 Would be nice if it read like sample ballot.
- 919 The sample ballot had numbers by the candidate names - since I was using a marked sample ballot it would have been faster to relate to the numbers.
- 875 Numbers on first page of sample ballot are no good. Sample ballot must be marked internally.
- 874 Should have the #'s the same as the sample official ballot. Takes too long to flip the chart to the names.
- 428 1. Needs to have numbers noted next to candidate/measure to confirm choices, I.e. Governor - 8 -Gray Davis- linked to ballot number. 2. Flashes noting " Next Contest" and "Please make your selection" stay on screen 2-3 seconds longer. 3. Confirmation
- 477 Need to have the ballot numbers also.
- 465 It should also give the numbers on the screen for each candidate.
- 449 Please put numbers of paper ballot same as sample ballot.
- 445 It would have been nice to have the numbers on screen next to the names and propositions, as they are in the sample ballot.
- 424 You really should warn voters to bring their ballot books - I usually have taken a slip of paper with No's for each item marked with my preference.
- 395 Put the numbers as they correspond with the book.
- 299 Numbers should be added to match the sample ballot.
- 286 Needs to be synchronized with official sample ballot booklet.
- 244 Like the sample ballot - Put #'s next to candidates & measures.
- 243 I can see many folks, especially older ones, having difficulties in doing this, understanding how to do it. On the propositions in particular, the Prop # are too small. Most mark dummy ballot by # of Prop in advance to save time in voting.

- 234 In developing the listing of candidates, measures and propositions, please include the numbers that corresponds to your choices on screen (like in the paper booklet). You may want use different color more creatively in denoting offices and measure changes.
- 223 Would like corresponding Nos. to match sample ballot.
- 1290 Place numbers correlating to voter pamphlet next to choices.
- 1269 I thought I liked the confidence of the No. and name of the Punch card voting- but this is OK- may be very confusing and difficult for other people.
- 1265 It might be helpful to have the ballot numbers on the screen for quick reference rather than having to read the tag of the screen to know where you are.
- 1261 Doesn't follow the sample ballot number system.
- 1225 A little fast to hasten "vote now" the mail out brochure has No's that are not available on screen.
- 1243 It might be helpful to have the item Nos. that are in the sample ballot document, included in each screen. Definitely needed to have my sample ballot document with me.
- 1245 Sample ballot and TC should display same number system for everything
- 1220 Listing the number with the name will help speed up the choice you want to make.
- 1205 The sample ballot numbers are not on the screen. It is rather confusing--the Nos. should be placed next to the name of the candidates.
- 1026 The numbers on my sample ballot did not show on the computer screen. So, my sample ballot on which circled the numbers was not as helpful.
- 379 I was confused about how to review selections. I liked that I could see actual names instead of punching numbers. I am a little hesitant about the mechanics- If I am doing it right - but I think that will change with experience.
- 373 I think it is much easier if #'s are next to the choices as this is how the sample ballots are printed.
- 319 Proposition numbers @ top of screen face need to be larger and bolder to make corresponding prop #. & title easier.
- 1002 Sample official ballots contain corresponding numbers to the vote, but machine does not. This may be helpful.
- 1155 Ballot number should be on the screen.

OTHER SUGGESTIONS AND COMMENTS

- 567 1. No place to put my sample ballot I had to hold it in one hand + vote with the other 2. Not enough privacy. 3. When vote for 2 out of several and 3 were max the box said" skip ballot" I wasn't certain my 2 got recorded.
- 548 Should put the numbers from the sample official ballot. I fill this in before. It would be great if I could use it.
- 555 If it could light up your choice when you touch it so you know that's the choice you picked, would be nice
- 559 The review part was confusing I didn't know where to scroll backwards to begin.
- 562 After inserting the ID card it came back but too fast and fell on the floor.
- 576 Glare on screen
- 577 I am worried that others can see what I am voting. Some old fashion curtains would be nice. Also at the end of the voting process there is no instructions how to use the scroll bar.
- 584 Picture or party icon identification.
- 585 Partition between machines
- 550 Last screen to conform selections only showed the bond measures. Instructions should indicated to scroll to see other selections.
- 509 The down arrow on the scrollbar on the left is too close to the cast ballot. You need a "Review choices" option @ the end w/o using the scroll bar. I would like some stud or ticket to walk away with.
- 530 People that don't usually use computers or ATMS etc. will need a lot more education's etc.
- 507 A little tricky when you have the option to choose up to 3 candidates and only decide to cast 2.
- 649 The header on item you're voting for should be designed so they stand out from the rest of the screen contents. The final step the review of what you voted for could be made easier . Explanation how to scroll back on what you voted.
- 643 it took a little longer to vote with the touch screen but provided the technology works properly I can vote with more confidence
- 627 wasn't clear on how to review all choices before casting ballot
- 802 arrange screen to eliminate glare! Raise level of paper read out.
- 818 would be better if it showed whole ballot in one copy (or at least didn't confine you to each selection, one at a time) so that it more resembles sample ballot.
- 690 receipt too small- needs darker ink.
- 603 I think we should vote in Election Day
- 607 machines were a little heavy for lap use
- 701 make review votes screen more plain- clear. Include ballot numbers on computer screen.
- 712 Hours need to be extended for working people. Possibly 2 weekends do not like sythetic voice. Need human voice. Switch does not give adequate volume. Problems with headset(broke and needed new one). Some Choices unclear when using escape button. At end o
- 711 When the screen message flashes to "cast ballot" over a persons name it could be very misleading. Someone could easily misvote for a person by pressing the "cast ballot" statement. The safeground of double checking the ballot at end of process in a good Idea
- 707 Raise the roof of the machine and make screen larger.
- 682 I found I needed instructions to find that I was to use the scroll bar on left to check entire ballot. Before finishing I found it very easy to check over what I had voted for as those instructions were very easy to see & use.
- 82 More details should be available regarding propositions & certain other ballot issues
- 73 It would be better if the screen world highlight the vote cast once you touch the screen. It wasn't quite clear.
- 69 Ballot & Screen was hard to relate if you used the summary sheet in front of ballot.
- 68 1. When a choice is made either it should highlighted or a beep should sound. 2. If you choose to skip context it should skip all example more then one candidate requires skipping multiple times.
- 67 Add a confirmation click sound when an item is selected.
- 46 Instead of hitting "Cast Ballot" twice. Have a "are you sure" questions.
- 44 Positioning of while voted indication should be on the name of the individual selected
- 11 It is difficult to read the headings at the top of the contest screens. Font should be bigger.
- 159 But being tall, I found the angle and glare a noticeable distraction. Particularly to have early voting in my workplace so not to have to go to the precinct
- 115 Need large scrolling arrows.

- 116 Put Election Day on Saturday or Sunday.
 999 Handicapped people need way to set chair, etc.
 151 1. Paper review (sensor should be worked on (longer time) 2. When reviewing appellate count candidates, their names weren't listed 3. Felt rushed with computer reminder
 135 System should not be used. It is subject to fraud.
 114 1. Would suggest note at the screen to indicate you cannot walk away from the screen. 2. Would like hard copy on paper of a different texture or color for the voter to take with him/her. 3. Have hard copy verification sheet at a higher location so that it
 143 after I pick a candidate, I would like confirmation of my selection before I proceed to the next one! Thanks!
 140 Did not show name for Judicial candidate during review. It show number (i.e. 2107) that was not on my sample ballot Blank card did not make me feel comfortable, as I did not know that was really my card.
 138 Not able to cast ballot with confidence. The choices need to have the numbers to match the sample ballot.
 974 #5. Wanted an "enter" button at the beginning.
 951 Compute put banner across screen too quickly when reading measure. I like the paper ballot better.
 941 I have macular degeneration of both eyes. Surgeries on one eye. I drive legally- read but need to move my head position to adjust to print, light and size of objects particularly in one eye. However, my diagnosis is macular degeneration of both eyes. This
 938 Probably more instructions for some people.
 937 Need to raise screen for tall people
 927 Auditory feed back when button is pushed would be good. Replace smiley face with flag or state seal.
 926 I liked it but it will take time getting used to.
 888 Print on top of ballot is a little small
 918 Please add seats.
 899 It presents problems for some groups- my mother (elderly) moved. Was very intimidated by the machine and get confused as to how she should use it.
 891 Would like for voting to be in mall.
 883 I waited until the last screen to attempt to review my ballot, but that was too late to review my first votes.
 908 User interface needs work to provide feedback to voter that they selected the choice they desired. I.e. The selections need to be "animated" in some way, either the selection flashes a few times or the selection box has an "inverting" button border to give
 497 Before final ballot is cast, there should be a review screen to show all final choices. Then offer to cast ballot and print selections.
 491 You should continue with demonstrations.
 858 More detail. Allowing the voter to view the entire ballot and details. Responses from candidates, etc.
 857 Would be good to have a practice computer.
 844 Voting for only 1 of 3 possible total unsure if "Skip" registered the vote cast.
 836 It will take one training every year they are used!
 830 I would like to review each vote before going to next item.
 827 The sample ballot needs to be easier to use if using a computer to vote.
 454 The sensor didn't allow the paper copy to be returned into machine.
 486 You must know who you will vote prior to coming to the booth, bring your sample ballot.
 446 Need more computers.
 436 Holder to catch card.
 416 Selected before touching.
 479 The review at the end is confusing. I could not tell how to review my whole ballot. I saw only a small part on the screen.
 483 The touch screen was difficult to register on some choices.
 484 #4 Not important. I found that the long ballot did not allow me to review earlier choices, since I was not aware of the ability to scroll back up.
 408 The "Trail" to the precinct not clear. Signs? The demo tape(instructions) to fast - not enough depth. My precinct average age of voter 60/65 Will the voter have a ledge to rest his sample ballot on?
 399 It repeated itself.
 400 #3 Headers
 403 Need to have a "go back" button after each selection instead of having to wait until the end.
 392 Please "redfeet" for people to stand on top so machine doesn't turn off.

- 291 Make scrolling easier to understand e.g.: when ballot is more than one page (screen), display instructions for scrolling.
- 289 You didn't know if you pushed the right selection. It doesn't light up. I didn't like the make a selection note when you take too much time making a selection.
- 285 1. Need to tell voter (on screen) not to step away from machine before finished. This causes big problems.
2. Confusion in second OK in "Cast Vote". 3. Confusion on statement in machine "Vote for 3" should read "Vote for no more than 3". 4. Flashing pro
- 393 I am an inspector for one of the precinct
- 273 Would like to have a brief summary/description of each candidate and/or measure.
- 272 I did not know how to go back to the beginning to check my voting.
- 252 #4 Speed is not a factor for me - being able to check over the ballot is much more important. I read Ginger Rutland's editorial column in the Sacramento Bee and looked for features she complained about. I agree the flashing "Please make your selection"
- 259 Final "Thank you" screen should remind vote to return card (smart) to poll worker.
- 253 I got confused at the beginning and tried to push my card in before I pushed a button.
- 254 The term "SkipContest" might worry some people if they don't want to vote for the max # of seats.
- 239 1. Unhappy that I did not get a receipt to prove I voted. 2. Big Flaw that you didn't put numbers that match the ballot next to the candidate name! Makes it take a lot longer! #3, Bad glare from lights.
- 240 1. Need to have one for handicapped with chair or ledge to put sample ballot on for referral or hand rails. 2. Big flaw that you didn't pout the candidate/measure numbers that corresponds with the Nos on the ballot!
3. Where's my receipt?
- 215 Being able to vote early made it so much easier - I forgot to ask for an absentee and this allowed me to vote. The touch-screen was great except I felt a bit rushed with the screen beeping at me and telling me to cast my vote.
- 1264 Proposition No. should be larger.
- 214 My only comment/recommendation would be to have each selection on this screen become highlighted, as it is chosen by the voter, so the voter can instantly see which choice he/she has made. I wasn't sure (until I reviewed my selections at the end) that I ha
- 1288 I would have liked to be able to read the issues to refresh my memory.
- 1284 Explanation should include situation of voting for only 2 when 3 (for example) is allowed.
- 1278 I wish you could see the entire ballot on screen for review purposes before you touch the "cast" button.
- 1262 Did not fully explain how to review ballot using scrolling buttons.
- 1238 Why not do it from home online. Create log on- etc. Do it from WWW.
- 1239 I'm into computers. I feel others might have a hard time.
- 1253 Associate justices names were not listed when I went back for review.
- 1191 In training need to show the up & down are in the "Review choices" screen. In the quick training this feature wasn't coured if the screen kept asking for a final decision. It may not be intuitive to a non-Windows user to manipulate the slide bar when only t
- 1188 Height needs to be adjusted and privacy needs to be addressed. Proof of voting-need stuff.
- 1168 21 yr. old.
- 1210 Some screens I had to touch twice for it to activate.
- 1213 Screen too low for tall people
- 1153 It would be nice to have titles for initiatives on the review screen. I would like to see candidate statement on screen.
- 344 #4: Is faster better? Security issues with potential fraud. However, voting early is nice.
- 358 Identification information at the top is very small and hard to read. It would also be a good thing to change colors each time it changes.
- 365 Hard to read the ballot below the machine. The proposition should have a bigger number so that you can vote using your sample ballot with ease.
- 376 Verification of elected office after touch prior to next office. Confirmation prior to screen change.
- 542 Josh Pane 916-737-2289
- 1001 I lived in Shreveport, LA for the 2000 Election, I liked their voting system, it was electronic, better. I prefer voting electronically, both in Sacramento & Shreveport, to manually voting.
- 10133 Needs to clarify how to go back into ballot to make changes or do skips.
- 1029 Pre-voting materials format (sample official ballot) will need to change. Otherwise it is about time. P.S. Computer scroll bars are on the right side, voting software should be the same for consistency.

- 1047 The survey form of 1047 contains two voter's comments. This is for one of the voters. The other voter's comment is put as 10470.
- 1050 Prefer optical scanned ballot, with ballot scanned immediately to detect over/under votes.
- 1051 If the system of what "Could Be" valuable timing for exposure and decision
- 1060 I fear hackers.
- 1066 Very light sensitive!
- 1142 It needs to educate the public a little more to be familiar with the machine.
- 1152 Movement sensor too sensitive

COMMENTS ON STAFF AND POLL WORKER SERVICES

535 The numbers of the propositions could be displayed in larger print for easier recognition of the proposition in question. Voting staff were friendly and helpful Thanks!

676 Lots of helpful people!

630 well staffed!

803 great experience + a helpful group of people instructing the public.

708 I would like little quieter location, however, overall the experience was pleasant and fast. John Ditty is an extremely competent and welcoming part of the experience.

10 Everyone was very helpful.

5 If the visual screen could change color confirming the choice touched before moving to next selection it would create less apprehension.

197 The pre-briefing was helpful.

955 Very helpful attendants

913 Found attending staff helpful

467 Good people. Keep up the good work.

451 Lots of good help on hand.

302 The staff was informational and great public servants.

1124 Every one is very helpful- fascinating

1229 The technical staff were a good assistance.

385 Crew was very friendly!

386 Volunteers were very helpful and friendly!

COMMENTS ON EARLY VOTING IN GENERAL

- 586 Early voting is good.
- 75 Less confusing than trying to punch the right hole. Thank you for offering early voting - I didn't have time on Nov. 5th.
- 66 I didn't have the chance to apply for an absentee ballot & I have to go out of the country & will be gone until after Election Day. This was a fantastic opportunity. The staff members were wonderful and very helpful!
- 203 My career doesn't allow me to always vote on Election day. Please continue early voting!!
- 190 It saves me from having to get up early before work on election day. This way I could vote near my work during my lunch hour.
- 131 This is a wonderful idea. I think people should have at least two weeks to cast their votes at convenient locations (near work).
- 118 Thanks KA
- 111 This is a much more convenient way to vote and I hope it will encourage more people to vote. There should be more location sin the future.
- 987 This is an easy and convenient way to vote. Hopefully it will be implemented throughout the county.
- 990 A great idea - I like the access at the mall- keep doing this!
- 922 Very excited to be able to do early voting at my convenience. It was wonderful to not to have a Nov. 5th time pressure. I am anxious for this convenience to be a permanent kind of way to vote. Thank you very much!!!
- 917 It's about time-- this is soooo convenient.
- 898 Please continue this process. It is just great! Thanks.
- 870 Need to have more advertising that this is an option. I do not like absentee voting but many times it is difficult to get to polling places. This is a great alternative. Thanks.
- 437 Way to go - Early vote is the future.
- 431 I enjoyed early voting and the convenience with a college schedule that does not fit with any work schedule, the early voting allowed me to vote on my own schedule.
- 423 I love having the convenience of having the early voting in a mall!
- 241 Early voting is great!
- 1292 I do not like my precinct to be mail in ballot only. I want the choice to vote in person.
- 1231 This was a great opportunity for me to vote early as I will be out of the county on election day. The system was extremely user-friendly and the demonstrator was patient and very informative.
- 1233 Great location for voting. It was a fast registration and voting procedure.
- 1234 I voted early today to try the touch screen machine. I like to go to the polls on election day.
- 1190 It was great being to register and vote all on the same day. The early voting is great for work too.
- 1189 Thought it was very convenient to be able to vote early and being able to register on same day voting!
- 1180 Great service!
- 328 Early voting was great for us since we are going to be out-of-town on that date.
- 312 Early voting to us a real blessing. System seems easy enough for anyone to use.
- 344 #4: Is faster better? Security issues with potential fraud. However, voting early is nice.
- 328 Early voting was great for us since we are going to be out-of-town on that date.
- 361 I hope early voting is permanent and near the communities, so the minorities can have a chance to vote.
- 1043 It was a surprise to vote so early and in the convenience of a mall in the morning on a Sunday. As a registered voter and recommend this. We live in a computer industries world. I am very impressed.
- 1183 When I lived in Texas the shopping center had polling booths in October for the convenience of voters. It enabled people who would not otherwise vote because of bad weather, bad neighborhood voting area or out of town to participate. I feel that having a fe
- 1158 Thanks to news. I found about the system and cast my vote early.
- 1159 This is the way to go. Thank goodness I can go on my cruise and know that I have voted.

B-3: WRITTEN COMMENTS FROM POLL WORKERS

The following points should be noted from these comments and suggestions:

1. The comments and suggestions are made based on the questionnaire posted by the County.
2. The groupings were made to facilitate evaluation.
3. Some of the concrete suggestions (some of them verbal rather than written) have been carefully studied and the following modifications have been or will be made to reflect the suggestions:
 - ⇒ The demonstration program should reflect the same “mechanism” and “flow” of the “real” election. This will be made in the future using the same contest/measure from the actual election but with “different names”.
 - ⇒ The electromechanical counters response to the “power-up” and “power-down” cycles have been isolated and corrected. The actual counts of vote after power-up and power-down were not affected in any of the systems.
 - ⇒ During the voter’s reviewing of their paper record, the sensor for “fleeing” voter was too sensitive. An additional sensor in parallel to the existing one will be added on the printer side. Any sensor detecting the presence of the voter will “inform” the voting unit that the voter is still nearby, and thus reduce the “sensitivity” or false-alarm by at least 100%.
 - ⇒ The video training tape will be reproduced to include all aspects of voting. This is particularly more important for full precinct voting deployment.

Sacramento Early Voting Oct. 15-25, 2002(AVANTE VOTE-TRAKKER™ EVC308)

Questions for Poll workers (18 Questionnaires were received)

1. SET UP
 - A. Did you find it easy to set up units on the first day of early voting?
 - 1) Set up became easier after the 1st day.
 - 2) Yes, our tech helps a lot on the setup and the system on Monday.
 - 3) Not difficult.
 - 4) Yes
 - 5) Mike did it.
 - 6) Yes
 - 7) Yes
 - 8) Skip
 - 9) Yes
 - 10) Yes
 - 11) No
 - 12) Yes

- 13) Yes
- 14) Yes
- 15) Not bad
- 16) N/A
- 17) N/A
- 18) N/A did not work that day.

B. Did you find it easy to set up units on each subsequent day?

- 1) Set up became easier after the 1st day.
- 2) Yes
- 3) Subsequent days fairly easy.
- 4) Yes
- 5) Mike did it.
- 6) Yes
- 7) Yes
- 8) Skip
- 9) Yes
- 10) N/A
- 11) Yes
- 12) Yes
- 13) Yes
- 14) Yes
- 15) Yes, easier and quicker
- 16) Yes
- 17) Yes
- 18) Yes

C. How much time did this take?

- 1) About 30 minutes
- 2) 30-40 minutes, mainly because @ sunrise we had to completely break down and lock machines & supplies in a small room.
- 3) First day about an hour, subsequent days about ½ hours. Daily setup somewhat hindered because we had to tear everything down and store it in a very small room.
- 4) ?
- 5) less than ½ hr.
- 6) ½ hr – 15 minutes.
- 7) 20 min.
- 8) Skip
- 9) About 30 minutes.
- 10) 5 minutes to activate machines each day.
- 11) 2-5 min.
- 12) 1st day 30 min. other days 10 minute.
- 13) About 10 min.
- 14) 15 min.
- 15) Usually an hour or a little less
- 16) By the end, it took about 1 hr.
- 17) 30-45 min.
- 18) 30 min.

D. Were your supplies easy to use/set up?

- 1) Yes.
- 2) Supplies were easy to use and ample.
- 3) Yes.
- 4) Yes
- 5) Yes, every day.
- 6) Yes
- 7) Yes
- 8) Skip
- 9) Good
- 10) Yes
- 11) Yes
- 12) Fairly easy. The blue seals were pretty low quality.
- 13) Yes
- 14) Yes
- 15) Not bad
- 16) Yes, buy we ran out of many supplies.
- 17) Yes
- 18) Yes

2. PROVISIONAL VOTERS**A. How did you like the provisional voter process?**

- 1) The process was easy.
- 2) OK
- 3) No problem
- 4) It is OK
- 5) Yes
- 6) OK
- 7) OK
- 8) OK
- 9) Good
- 10) Plastic is simple and votes are easy process
- 11) Easier than reg. polls!
- 12) Fine
- 13) It was quite simple
- 14) Skip
- 15) More complicated but manageable
- 16) Skip
- 17) Yes
- 18) Very easy

3. MULTIPLE LANGUAGES**How did you like the process for selecting one of the two languages?**

- 1) Skip
- 2) Yes
- 3) Fine
- 4) V. good
- 5) OK
- 6) Good
- 7) OK
- 8) OK
- 9) Yes
- 10) The ballots need to be available in all major languages in use in Sac. County. Voters other than those who legally use Eng. Or Spanish need to be better accommodated.
- 11) Good start.
- 12) Skip.
- 13) Easy
- 14) Yes
- 15) Great
- 16) Skip
- 17) Skip
- 18) Great

Did voters seem to understand this process?

- 1) The majority of voters understood the process.
- 2) Don't believe we had anyone use other than English

- 3) Yes, can't say anything but English was used.
- 4) Yes
- 5) Yes
- 6) Yes
- 7) Yes
- 8) OK
- 9) Yes
- 10) Skip
- 11) Yes
- 12) Easy to understand
- 13) Yes
- 14) Most
- 15) Yes, and liked it.
- 16) Skip
- 17) Touch screen on (English) not OK.
- 18) Yes

4. OUTREACH

How much cooperation did you get from the vendor for setup and breakdown of the system, and did they assist with voter demonstrations?

- 1) Vendor assistance was very good.
- 2) Yes indeed. Everyone from the vendor was quite helpful and easy to work with.
- 3) Vendor very helpful – yes if necessary.
- 4) Good cooperation
- 5) Mike did it all. He was great. Yes they assist with voter demonstrations all the time.
- 6) Lots of cooperation, lots for setup and breakdown and yes they assist with voter demonstrations.
- 7) He was great.
- 8) Yes
- 9) Yes
- 10) 150% cooperation from vendor staff.
- 11) Excellent, could not ask for more assistance than received.
- 12) Yes, they were a big help.
- 13) A lot- big help.
- 14) When they were around they helped out great!
- 15) Tons, great help from John and Kevin and especially Dave. Yes, always handy, volunteered but never “stepped in and took over”
- 16) No comment
- 17) Dave is great help.
- 18) They did a great job overall.

5. CLOSING THE POLLS

Do you like how this system suspends during each night of early voting?

- 1) The procedure was easy
- 2) Yes

- 3) Satisfactory
- 4) It is OK
- 5) Yes
- 6) Yes
- 7) Yes
- 8) Yes
- 9) Yes
- 10) Yes
- 11) Yes
- 12) Yes
- 13) Yes
- 14) Yes
- 15) Yes, easy
- 16) Skip
- 17) Yes
- 18) Yes

Do you like how this system closes at the end of early voting?

- 1) The procedure was easy.
- 2) Was not working last day.
- 3) Satisfactory. Because we were in an open mall we had to break down and put everything in a locked room. Would be nice to be in a room that could be locked.
- 4) No opinion
- 5) Skip
- 6) Yes
- 7) Yes
- 8) OK
- 9) Yes
- 10) Yes. This all eliminates the long, slow process that manual voting systems require.
- 11) Yes
- 12) Yes
- 13) Yes
- 14) Skip
- 15) Yet to do this but appears easy.
- 16) Skip
- 17) Yes
- 18) Yes

6. What difficulties did you encounter interfacing to the vendor's database system?

- A. DFM (EIMS) – for looking up the voter and issuing the absentee ballot
 - 1) Works very well
 - 2) The system booted us out quite often. Sometimes we had to completely turn the laptop off and start over to get back in.
 - 3) The only problem we had was computer shut down and label machine very slow.
 - 4) Did not do this
 - 5) None, the system was great

- 6) None
- 7) None
- 8) None
- 9) Good
- 10) None
- 11) 95% approval
- 12) Skip
- 13) No problem
- 14) None
- 15) Several times went "off-line". Each off-line took couple minutes. Saturday 5:15 could not get back online. Had Don from office come out.
- 16) Skip
- 17) Great
- 18) None

B. AVANTE-for looking up the precinct and programming the card

- 1) Very well
- 2) None at all
- 3) Programming of card no problem
- 4) Did not do this.
- 5) The system was great.
- 6) None
- 7) None
- 8) None
- 9) Good
- 10) None
- 11) Easy, simple
- 12) No problems, very easy
- 13) No problem
- 14) None
- 15) None, no problems
- 16) Skip
- 17) Great
- 18) None

7. How did you like using laptops?

- 1) OK
- 2) Very much- but sometimes the system was very slow. We were disconnected a number of times – sure learned how to get back in.
- 3) Great
- 4) Alright
- 5) Yes, they were fine.
- 6) Great
- 7) Good
- 8) Ok

- 9) Good
- 10) Yes, more may be necessary to accommodate polling places with large voter turn out.
If for no other reason, additional laptops should be at polling places back up if a computer crash should happen.
- 11) Easy to use and convenient
- 12) Good, very easy.
- 13) The laptops were quite simple to use.
- 14) They were easy to use.
- 15) Fine, but use my own (DELL) regularly so use to laptops.
- 16) Skip
- 17) Great
- 18) Very much

8. How do you feel about the sites selected for early voting?

- 1) The sunrise site was very good.
- 2) Skip
- 3) Traffic areas needed and malls are as good as any.
- 4) Fine
- 5) SOS was great
- 6) Good
- 7) OK
- 8) No opinion
- 9) Great
- 10) Public places with large volume of traffic should increase the number of voters who participate in the election process.
- 11) Florin mall has less traffic than other malls.
- 12) Good sites. Hopefully will be more next time.
- 13) They seemed like very good sites where a lot of people would be.
- 14) Skip
- 15) Market square was great (worked there) Sat with sunrise a couple hours – OK spot but out of traffic area. Florin spot was also out of walking traffic.
- 16) Skip
- 17) Great location, market sq.
- 18) It was great, lots of traffic

9. How do you feel about the printed receipt?

- 1) Skip
- 2) Skip
- 3) Skip
- 4) Works
- 5) Skip
- 6) Not sure
- 7) OK
- 8) Skip

- 9) Good
- 10) Skip
- 11) Skip
- 12) OK
- 13) Skip
- 14) They are good because it make the voters more confident
- 15) Think it's a good idea
- 16) Skip
- 17) Skip
- 18) A little slow, but great.

A. Did voters seem to like it?

- 1) Yes
- 2) Yes, but they wanted to keep the receipt and thought they should
- 3) Many complained about the readability of the receipt. Too low bifocal problem, small print.
- 4) Yes
- 5) They felt they should take it but were OK to leave it.
- 6) Yes
- 7) Yes
- 8) OK, but wanted copy
- 9) Good, yes
- 10) Yes, many wanted a copy for themselves.
- 11) No records, voters wanted a copy
- 12) So-so. Some wanted to keep it, but not a problem.
- 13) Yes
- 14) Yes
- 15) Yes, most want receipt to carry away after voting.
- 16) Skip
- 17) OK
- 18) Yes

B. Were there any problems with emptying the tray?

- 1) Sometimes ballots would get stuck.
- 2) Did not do this.
- 3) No
- 4) Some
- 5) Skip
- 6) No
- 7) No
- 8) Skip
- 9) Yes
- 10) No
- 11) No
- 12) No problems
- 13) No

- 14) No
- 15) Once-ballot stuck in front, out of tray. (needed long "tongs" from nearby food court to snag and remove it).
- 16) Skip
- 17) Skip
- 18) No

10. Would you do this early voting again?

- 1) Yes
- 2) Yes, also many voters spoke favorably about being able to vote early.
- 3) Yes
- 4) Yes!
- 5) Yes
- 6) Definitely
- 7) Yes
- 8) Yes
- 9) Yes
- 10) Yes
- 11) Yes!
- 12) Yes
- 13) Yes, it was very simple and everyone seemed to enjoy it.
- 14) Yes
- 15) Yes, definitely
- 16) Skip
- 17) Yes
- 18) Yes

11. Is there a procedure (or procedures) that you would change to better facilitate this process?

- 1) Once understood, the procedure seems to work well.
- 2) Skip
- 3) Yes, why say the voter can read the receipt to verify their vote. They already had two chance to review their ballot.
- 4) Yes
- 5) Make scroll bar easier to use.
- 6) No
- 7) No
- 8) Scroll bar on right like all computers. Public want numbers by names that coordinate with sample ballot numbers.
- 9) Numbers
- 10) Sign is important at each site. Media should be more involve in promoting the process and make it clear that any registered voter can vote at any polling site.
- 11) A work in progress
- 12) No

- 13) No
- 14) Skip
- 15) Better laptop connections & simplify. Voters would like receipt. Voting machines worked great but bulky & bit heavy for setup.
- 16) Skip
- 17) None
- 18) No

ADDITIONAL COMMENTS

Get the word about early voting out to more people.

Voters would like to see numbers also to have screen just like the ballot book.

There need to be clear directions/instructions as to the function if each poll staff work

Data entry clerk (1) registration

Data entry clerk (2) encoding of card to activate precinct information on voting machine.

Voter assistance clerk, assists voter in beginning the voting process

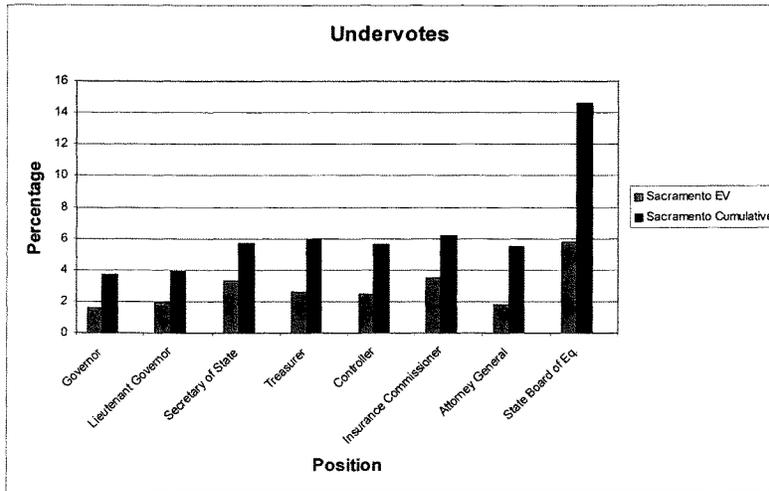
Inspector should be able to perform all tasks.

ATTACHMENT C

**COMPARISON OF EARLY VOTING UNDER-
VOTES OF THE VOTE-TRAKKER™ SYSTEM
WITH THE CUMULATIVE UNDER-VOTES
(COMBINED WITH PUNCH-CARD VOTES)
FOR SACRAMENTO, CALIFORNIA 2002
GENERAL ELECTION**

C-1: UNDER-VOTES COMPARISON BETWEEN VOTE-TRAKKER™ DRE TOUCH-SCREEN SYSTEM AND PUNCH-CARD SYSTEM USED FOR 2002 GENERAL ELECTION IN CALIFORNIA

(An under-vote is cast when a voter does not make a choice on the specific contest.)



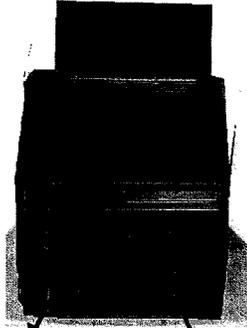
ATTACHMENT D

**CONFIGURATION COMPARISON OF
VOTE-TRAKKER™ MODEL EVC308
AND EVC 328**

D-1: EVC308 vs. EVC328

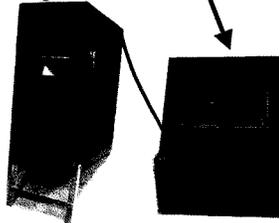
HARDWARE

- ◆ Real-time ballot record printer separated from voting module and housed in its own case.
- ◆ Printer module can be swapped out without compromising voting module integrity.
- ◆ If counties or jurisdictions so choose, the printer and voting module can be attached to each other as a unitized unit as well.



EVC 308

All components are the same and incorporated into the EVC328 into a modular design.



EVC 328

- The EVC 328 can be used without the real-time ballot record printer if so chosen by the jurisdiction.
- A small thermal printer is an option and located inside the unit to create tallies and zero reports.

SOFTWARE

⇒ The same software runs on either EVC308 or EVC328.

JILL LAVINE

BIOGRAPHY

(Current: 7/2/03)

**Director (Registrar of Voters)
VOTER REGISTRATION AND ELECTIONS**

County of Sacramento
7000 65TH Street, Suite A
Sacramento, CA 95823-2315

Telephone: (916) 875-6558 FAX: (916) 876-5130 E-mail: LaVineJ@saccounty.com

**EMPLOYMENT
COUNTY OF
SACRAMENTO,
CALIFORNIA:**

REGISTRAR OF VOTERS

(Aug. 3, 2003 - Current) Responsible for entire operation of the Department of Voter Registration and Elections

Extensive historical knowledge and experience of the complete election process, through the 17 years of service, as a result of progressively responsible duties and various positions assigned in the following capacities:

Assistant Registrar of Voters
Election Manager
Election Assistant
Election Clerk

Committee Leadership: -Request For Proposal (RFP)--Evaluation Team for New Voting System
-Budget Process
-Spanish Advisory
-Postal Liaison
-Sacramento County Redistricting--(Reapportionment)--(after the 1990 and 2000 U.S. Census) including mapping and presentations to communities and Sacramento County Board of Supervisors

Project Management: -Early Voting Implementation, Nov., 2002 General Election, County of Sacramento, CA
-Sacramento County Voter Registration and Elections Outreach

Business Management: Certificate, TQM (Total Quality Management)

MEMBERSHIPS:

CACEO *(California Association of Clerks and Election Officials)*

Co-Chair, Election Legislation Committee, 2004
Subcommittee Member, Recodification
Subcommittee Member, Voters with Special Needs
Subcommittee Member, Help America Vote Act
Subcommittee Member, Petitions

THE ELECTION CENTER

Member
Speaker, National Conferences
Graduate, CERA (Certified Election and Registration Administrator)--(1996)

NACRC *(National Association Of County Recorders, Election Officials And Clerks)--(An affiliate of NACo--National Association of Counties)*

The CHAIRMAN. This was also shown. This is from Maryland. And this was the printout from it. And I would note that I did see the name Hoyer nine times, so I thought I would mention that.

Mr. HOYER. Mr. Chairman, if I could, I want to apologize to Attorney General Lamone—that was some years ago—for missing her testimony, although I have a reliable report that it was excellent and right on point. And I thank you as well, the two of you who have not the theoretical discussion but the practical problem of confronting hundreds, indeed thousands, of voters and ensuring that they are processed in a way that gives them confidence and does not discourage them from voting and has voting occur in a time frame that can handle a large number of people.

Let me say, Dr. Rubin is also here. Mr. Kohno, the graduate student, is here as well. I think Mr. Williams and Dr. Shamos have left.

Mr. Chairman, you and I have had this discussion. This is not an adversarial proceeding. This committee worked together—Mr. Ney and I, Mr. Larson was very helpful as well, Mr. Dodd and Mr. McConnell—to try to facilitate voting and to give voters a greater degree of confidence that they could vote accurately and that it would be counted. We did not mandate a technology. We purposely did not mandate a technology.

We did mandate that you could not use Federal dollars to replace a lever machine or the punch cards because, A, the leverage machines have essentially gone out of business with no replacement parts; and secondly, the punch cards have proved to be one of the least reliable systems; although, as all of us know, paper ballots themselves are very high up on the list. If you had just the paper ballot system, they are higher up on the list of mistakes as well.

We all want to get to the same place, and that is a system where the voter has confidence, the jurisdiction, whether it be a county, a State, or a country, has confidence that as a result that is what the voters intended the result to be.

I think we can do that. I will tell you, I don't think we can do it between now and November in terms of the technology that will be available.

So what the Chairman was saying and I think what Mr. Larson said as well—and I apologize. I apologize. I give a press briefing every week. But we want to make sure that no voter in America this year is discouraged from voting. We don't want to undermine their confidence.

My problem as, Dr. Rubin, you have probably read, and Senator Dodd's problem is not with the analysis, because you are an expert and we are not, and we ought to make sure that whatever technology we use is not subject to being manipulated and is accurate and fair; but that the debate that is occurring concerns a number of people, not just those with disabilities, who are concerned that we will go to a system that does not provide them as for the first time in history they have been provided with a mechanism to vote secretly.

Mr. Dixon was in the room, as you know. Mr. Dixon is blind. He is a wonderful person, a bright, knowledgeable, able person, and he like every other American wants to go into a ballot booth and vote,

and he wants to know how he votes, and nobody else, unless he wants to tell them.

Mr. Ney, myself, Mr. Larson, and Senator Dodd and Senator McConnell were pleased that we mandated that that happen. This technology, DRE technology, is one of the ways both from a visual and/or audible standpoint that allows that to happen.

What I am hopeful, Mr. Chairman, is that we proceed in a manner which will give Americans confidence that we are pursuing the best technology we can possibly find, using all the expert advice and counsel. But at the same time, while we are evolving towards whatever system we arrive at—and my presumption is that this process will always be evolving because we will get better technology and better security and better ways to do things, and that is progress—but that we not get so animated in our debate that we undermine citizens' confidence. That would not be a result that I know any of us seek.

So I apologize, Linda, that I didn't hear your testimony. I will read it.

And, Ms. Rogers, thank you very much for what you and Georgia have done. Georgia and Maryland were two of the leading States in terms of trying to adopt technology.

I want to say, Mr. Chairman, in closing, that—Mr. Ehlert unfortunately has left, and I didn't want to interject at that point in time—we do need more money for NIST. I would like to offer an amendment, adding \$2.8 million, which is what NIST says it needs, to the NIST budget in the Commerce, State, Justice. You and I have had that discussion. The budget is so tight. I would like to have them—they get 300-plus million; 2.8 million of that I would like them to use in the short term, because this is an immediate problem and this could be helpful to us. And Mr. Ehlert was primarily responsible for NIST being a part of HAVA. And I think Mr. Ney and I both believe that that was a very positive suggestion.

But perhaps we can work on that because, again, this is not an adversary relationship. Everybody wants the same objective. Everybody. And in that context, as I was telling my good friend Rush Holt, in that context, people of goodwill, experts and practical appliers of technology, we ought to be able to get together and figure out how we can do this, but in the interim do the very best we can, which in my opinion is going to be far better than 2000.

There are a lot of other things in HAVA: second-chance voting, provisional ballots. We are not there yet. But when we get to on-line statewide registration, interfacing with local precincts, that is probably going to take us the longest time and be most expensive in the long run, probably, but that is a wonderful reform: accessibility of all polling places.

There are some wonderful things in HAVA which do not deal directly with the technology question, but giving jurisdictions the ability to afford—Mr. Mica, I disagree with Mr. Mica very fundamentally. The Federal Government has been on the State dole since 1789, which means that for over 200 years, we have not contributed a nickel to the running of Federal elections; \$3.9 billion is a small sum for us to help 55 jurisdictions, 50 States, the District of Columbia, in doing what they have had trouble doing, because so often they were the last people considered in the budget process,

because elections just seem to be, well, we are working and we are stumbling along. HAVA was an attempt to try to empower the States to bring our elections up to date and to utilize the technology available to make sure that we accomplished the objectives stated.

And, Mr. Chairman, I know you and I are in 100 percent agreement that \$3.9 billion is a small sum, relatively speaking. It is how much money we will spend in Iraq. I supported the authority and I believe our mission in Iraq, if accomplished, will be a very positive accomplishment. But it is more money than we spend—it is less money than we spend in Iraq in 25 days to make America's democracy work better. A good investment.

The CHAIRMAN. Thank the gentleman. And I want to ask some questions, but I do want to make a statement first, too. You know, the Help America Vote Act went way beyond the hanging chads. And I will be frank with you, and I know that Congressman Hoyer heard this, I heard it; many asked, why do you want to do something? Let it go. We can't afford it. We shouldn't do it. We shouldn't change the system.

And I didn't know this until the Bush-Gore election, that 1,800-some votes weren't counted in my own congressional race. Now, it didn't matter because the margin was so big. But if it had been close, there would have been 1,700 individuals that would not have been in the process, would have been disenfranchised. So I think something had to happen.

HAVA wasn't done on a whim. We would have liked it to have passed faster. But the process took time. And that is the way things run. But we reached out also in that bill, Carter—the Ford-Carter Commission, they contributed to it. We talked to the NAACP, we talked to election officials, and we reached out to others. We didn't do it in a vacuum or behind a closed door, and we especially talked to people on the front line, like all of you. You are on the front line. You can do good research or people can do science projects when it comes to these issues. But the fact remains that you are out there and you see how the voting system actually works.

That doesn't mean we take this issue lightly or take the bill lightly. And we don't take the lack of funding lightly either. And I am hoping within one of these bills—and I think what Congressman Hoyer said is completely correct and accurate—we will work toward fully funding HAVA.

As far as the money goes, when this started we went to Speaker of the House Hastert, and then Leader Gephardt, and sat down with both the Speaker and Leader Gephardt. Money was not an issue. We spend \$5 billion helping blossoming democracies around the world, and that is great. So I don't think \$3.9 billion is too much to spend on improving our democracy here at home.

And what the Congressman wants to do is critical to securing that money, at least here in the house. And frankly, I don't think any of us will rest, and that includes our Senate colleagues, until we get all of the money; because you should have some resources, which the Federal Government has never before provided.

I think I am going to ask a question. Unfortunately, this whole debate, and I think most all of you pointed this out, there is some

unfortunate twisting that has happened. A lot of things have been overshadowed. Comments have been made about individuals who run these voting system companies who have supported a Presidential candidate. That is unfortunate that ever happened. We have to move beyond that and look at what is going on. And the Election Commission can try to devise ways to look at the security of these systems.

I know the paper ballots weren't working. And, again, the main problems our election system has faced throughout the history of this country have involved paper. But I know the intentions of election officials—and you did watch in your States for situations, and you did monitor your respective election systems. And I think a lot of you have been maligned unfairly, frankly. It has been twisted. There are people involved in this debate for the right reasons who are doing good research. And there are people in the front line. I think that is why this hearing helps, and helps get issues out on both sides of this issue.

Mr. HOYER. Mr. Chairman, would you yield a minute? One of the things I mentioned, registration. One of the statistics that was brought before us when we had the hearings on HAVA was that many more millions of people lost their vote because of registration issues and technology issues by far, by a multiple of maybe 3 or 4. I don't think there is a precise number obviously, but significant. And we ought to keep that in mind, because as the Chairman said, HAVA has done a lot of things in addition to this and this is getting all the attention.

But I am hopeful we get voters—I know the election officials are—but you run the system with 95 percent volunteers on one day, it is tough not to make mistakes because it is a human factor. But second-chance voting is essentially new, and provisional ballots are new, and there are paper ballots and they have to be set aside and have to be checked to see whether or not the voter actually is—and I am concerned, Mr. Chairman, there are different State laws. In HAVA, we were focused on not empowering the States and not limiting the States, but I am not so sure we didn't make a mistake by having State law apply; because some States say if you don't live in that precinct, even if you may be voting for all the same people as voting in the next precinct, you can't have a provisional ballot. I think that is unfortunate.

I don't what the law is in Georgia and I don't know what our law is on that, Linda. But in any event, registration is one of the huge problems that we are not as focused on because we are so focused on technology, and many more millions lost the opportunity to vote because of registration issues than because of technology, hanging chads, or other technology issues.

Thank you, Mr. Chairman.

The CHAIRMAN. Two quick questions. I know the Ranking Member will want to ask questions. What potential unintended consequences could result from mandating that all DREs be equipped with a paper trail?

Ms. ROGERS. I would be happy to share with you myself, and I believe Jill as well, I began my career in elections as an elections worker in the polls way back in the early eighties. And I can tell you through all my years I worked in the polls with lever machines

and I worked with optical scan equipment, I firmly believe that the introduction of paper into the polling place on a busy Election Day is going to cause mass confusion. It is going to upset voters who don't want attention called to them if there is a problem. Voters like the ability to stand at a unit, review their ballots, such as they do with electronic voting. It shows them what they have voted prior to touching cast ballot, and they do that in private.

When you vote on an optical scan-based system and you walk over to put it into the machine, if that ballot has been overloaded, it kicks it back and might read on the little LCD, and it might say "overvoted race 10." Well, you have got a line of voters standing behind you and you, the voter—the poll worker says, Would you like to take this over and correct it? Correct what? It is intimidating to the voters.

I am very afraid the paper receipt such as you saw in the demonstration a little while ago would be mass intimidation to voters, and I believe the very same to poll workers just based upon—and that is based upon my own experience as an elections official. The introduction of paper is going to cause a great deal of heartache and headache.

The CHAIRMAN. Just a scenario here, because it comes to mind when you are talking. If I get my receipt and I am in the privacy of the booth, I take that receipt, right? I would have to go outside.

Ms. ROGERS. You would actually take the receipt and then deposit it into a box on your way out the door. Now, that scenario gives me a lot of concern, because what is going to happen when the voter says, You are not having this receipt? What does the poll worker do then? In other systems, it sort of sucks it back up into the machine. And given the length of what you saw, I have seen some that develop that is a 4-inch window plexiglass. This roll of paper would move behind the glass and it does 4 seconds where you see the 4 inches at one time. So the voter would have to quickly view that as it is going around, and then it would have to not get caught or jammed in the system. But there are two different components: one you would drop in the box, and one would stay behind glass.

The CHAIRMAN. If I get that in the privacy of the booth and I come up and you say, Where is your receipt? And I say, It didn't spit one out. And you say, It had to. And I say No, it didn't; are you calling me a liar? And I put it in my pocket.

Ms. ROGERS. Which could easily happen. That is one of our greatest concerns over paper receipt.

The CHAIRMAN. The other question is, do you believe the mandatory paper trail would increase the system security? Does it add anything to security itself?

Ms. LAMONE. No, it doesn't in my estimation. I think what Dr. Shamos said earlier was that testing, testing, testing. And his idea of having standards that are well thought out and not voluntary, I think is the way to go. Maryland law requires us to adhere to the Federal standards. I have no choice, and I do not rely on the ITA report solely for our security analysis. I think it would add more trouble than, frankly, what it is worth.

There is emerging technology out there, whether it involves a piece of paper that the voter can then go and verify post-election

that their vote was accurately counted, but it is all encoded, it doesn't have names on it. And there is also some electronic technology that is coming about that would provide us with a better opportunity to audit the election and make sure that the equipment was performing.

The CHAIRMAN. You know, I remember speaking with one of the companies that produces voting systems. This company doesn't produce a receipt and they don't want to produce a receipt. But one of the companies that I saw in a meeting told me, Look, we can produce a receipt. We don't think it ought to be used though. We don't think that that gives the security that people believe it will.

And so therefore, that is why I think we should take this seriously and we should have some ability to check machines to see if there is fraud, which you all have done, including in Maryland, where you haven't gotten credit for it, but you have done it. But we should do that, because the movement now has been towards, well, forget machines, this should be all paper.

Isn't it true, too, if you could manipulate the machine, you could manipulate the paper? If you fix the machine, the paper comes out. So it is still an issue, the machine's integrity, which we should take seriously.

And wrapping up my questions I have for Ms. Lavine, just about that pilot which Sacramento County used, the DREs, which produced a voter-verified paper trail. The pilot took place during early voting prior to Election Day.

Ms. LAVINE. Yes, it did.

The CHAIRMAN. Would the conditions have been different if it had been an Election Day, do you think?

Ms. LAVINE. We were going to just to try the system. We didn't want to do a full rollout in every single polling place. We wanted to keep it controlled. That is why we only had it for early voting in certain locations. We were able to have an authorized technician from Avante at each single polling place. And if we had done a full rollout on Election Day, there was no way we could have had a technician at every one of our polling places.

The CHAIRMAN. You had six polling places, so you could have six technicians?

Ms. LAVINE. Yes.

The CHAIRMAN. How many polling places do you have in the county?

Ms. LAVINE. Normally over 800.

The CHAIRMAN. You couldn't have 800 technicians.

Ms. LAVINE. And we wouldn't have had that many experienced personnel either. We staffed from our office to make sure we had someone there that knew the ins and outs.

The CHAIRMAN. How much longer did it take to vote in these six polling places?

Ms. LAVINE. It didn't take that much longer to vote. It was the verifying of the receipts. But most voters who were in a hurry—many voters didn't want to stay, and left. So they just said, No, I am not interested, go ahead and do whatever you want to do with it.

The CHAIRMAN. You said 127 hours?

Ms. LAVINE. One hundred twenty-seven and a half hours to verify. We did the manual recount verifying what was the paper versus the electronic. And when you pull out those long pieces of paper, they start curling like Goldilocks' curls, and you are holding down both ends. We did them in teams of two to verify the electronic count. To read back and forth and no way to quickly read the paper ballot, it took that long to verify only 114 of the ballots. We didn't do the entire project.

The CHAIRMAN. How many ballots were included in the six polling places?

Ms. LAVINE. One thousand six hundred twelve ballots.

The CHAIRMAN. What would you have on an Election Day?

Ms. LAVINE. Close to 300,000.

The CHAIRMAN. Why was the system not adopted?

Ms. LAVINE. There are many things. At that point, the Secretary of State had not come out with his decision on whether it was necessary to have the paper verified, voter-verified paper audit trail. We cancelled the RFP that we were in the process of, and we were waiting for things to settle down a little bit to see which way the wind was blowing.

The CHAIRMAN. If you had a thousand ballots, it took 127 hours. Statistically, it would take how long? Just a guesstimate.

Ms. LAVINE. I didn't figure that one out.

The CHAIRMAN. I would assume a long time.

Ms. LAVINE. Longer than the 30 days that we have to verify an election.

The CHAIRMAN. For a thousand ballots—how many ballots do you normally get?

Ms. LAVINE. I am sorry.

The CHAIRMAN. You have a thousand ballots.

Ms. LAVINE. Only 114 ballots that we counted.

The CHAIRMAN. And it took 127 hours? If you add 3,000 it could take months.

Ms. LAVINE. We have 300,000.

Ms. LAVINE. Years.

The CHAIRMAN. Years.

The CHAIRMAN. Mr. Larson.

Mr. LARSON. Let me thank you for your enlightening testimony. And before I ask just a couple of rudimentary questions as they relate to the monies, I want to go back and emphasize something that our distinguished leader said, Mr. Hoyer, that in looking at this issue, it is especially intriguing from a scientific and technological aspect but equally compelling in terms of the practicality of putting these things into practice.

I want to commend Dr. Rubin. He said in his testimony in weighing what we have all been discussing this morning, his duty and responsibility to speak out, and I commend him for that because I think that is what enriches our process. That is what allows us to get to the heart of the matter.

And the first panelists—the goal was, from my perspective, was to lead people towards a practical consensus. I think it has been further enhanced by your testimony this morning. My questions deal specifically with the monies that you are receiving and have been appropriated under HAVA. Have they been fully utilized and

are they helpful and how will they relate to what we talked about before in terms of training—which, Mr. Hoyer called you Attorney General Lamone—but how do they relate to how you have been able to—you gave elaborate examples of everything that Maryland has done and I assume Georgia has done. I am concerned how this money—and of course, I share with Leader Hoyer and our distinguished Chairman the concern about getting additional monies out there to accomplish what I believe was the consensus of the first panel, that what we need is testing, testing, testing, training, training, training. But conceptually, I had thought about when we were talking about a paper ballot, I thought we were talking about a card, something that was readily available and handy. And obviously your demonstration of about a 10-foot long paper ballot and all the ensuing problems that that creates is a compelling visual demonstration that deals away from the common idea; because you know, we have been comparing this verbally to receiving a receipt from an ATM machine, which is quite different when you contrast this. Not that I don't think technologically that could be overcome in the future, but we are dealing with the practicality of a November election.

So my questions are: One, the monies that you are receiving; how are they being expended? Are you utilizing them? I have a special question for California, because we did have the opportunity to meet with Secretary of State Shelley, and Leader Pelosi arranged everything. Mr. Hoyer and myself were able to go to that. And I know there was a question of decertification, but Mr. Shelley went to great lengths to say that, yes, but he did that so there would be an opportunity to correct the—what was wrong, what they had detected as being wrong with machines. And I want to know how that process has gone.

We also heard some indication from Georgia that some of the monies that were coming down from HAVA might be used by the State to address Medicare issues. And I want to know if that was something that was misreported. But I do think—especially given the scarcity of funds and the need for us to focus on this issue, how that is all taking place. If you care to respond.

Mr. HOYER. Thank you for allowing me to participate. Unfortunately, I have to leave, but I want to thank you and Mr. Larson for your leadership on this issue. And I think these hearings are important to see what we have done and what we are doing and what we need to continue to do to accomplish the objectives. And I want to thank all of the witnesses, who I think were all very good witnesses. Good information, and we will digest it and take such action as we deem to be appropriate.

[The statement of Mr. Hoyer follows:]



For Immediate Release
July 7, 2004

Contact: Stacey Farnen
202-225-3130

**HOYER STATEMENT ON
HOUSE ADMINISTRATION COMMITTEE HEARING
ON VOTING SYSTEMS**

WASHINGTON – House Democratic Whip Steny Hoyer released the following statement today regarding the House Administration Committee hearing on voting systems today. Congressman Hoyer was the lead House Democratic sponsor of the Help American Vote Act of 2002, the landmark election reform legislation.

"I applaud Chairman Bob Ney, Ranking Democrat John Larson, and members of the Committee on House Administration for inviting the distinguished panel of election officials and technology experts to help educate the American people on the security and performance of voting systems, an issue that has attracted considerable attention in recent months.

"As the committee of jurisdiction in the House on election-related issues, the House Administration Committee is in the position to gather the most current information on voting technology and pose tough questions about voting technology.

"I believe that this hearing will help us reach a sober judgment regarding the reliability of the voting systems that will be used in November's election and what steps, if any, should be taken to make sure every vote cast is counted accurately.

"Voters deserve to know that this year's election will not be a repeat of the controversial 2000 election. They also deserve to know the technology they will be voting on is secure and accurate. And I am hopeful that this hearing will advance those goals."

###

The CHAIRMAN. If it wasn't for your perseverance, we wouldn't have the bill.

Ms. LAMONE. I will go with the first question. I think I can state for every jurisdiction in the country and the territories that the money is more than welcome, but it is not enough. The unintended consequences of what is going on with this discussion about security and training, testing, and so forth, at least in Maryland, I am expected to use the Federal money first. So here we have got all these other things we have got to do under HAVA, 13 different mandates, and I am sapping, I am draining the money, the HAVA money off to do all this other stuff that I don't think anybody anticipated a year and a half ago. That is not to say it is not important, but it is unfortunate because I still have major projects to do, namely the voter registration system.

There is going to be a time of reckoning, if there are no more Federal dollars appropriated, when the State is going to have to cough up additional funds.

Mr. LARSON. And the voter registration problem is one that Mr. Hoyer points out where the greatest number of people ended up being turned away from voting; is that not correct?

Ms. LAMONE. Yes. Nationally, that was correct. I am not sure that that is the case in Maryland. But we do think differently in Maryland than some of the other jurisdictions.

But to answer your question, we got a lot of money and it is not going to be enough anyway, and we are being forced to use it for unintended expenditures.

Mr. LARSON. If I could play devil's advocate and be Mr. Mica for a second, what is enough money in your estimation? What would Maryland need?

Ms. LAMONE. I think the Department of Legislative Services, which is the advisory group for our Maryland General Assembly, estimated between 100 million to 130 million for Maryland to complete all the tasks and make the payments in the outyears. It is a little bit over twice of what we have gotten.

Mr. LARSON. Would the same be true for Georgia?

Ms. ROGERS. We believe if we were to receive the full funding that HAVA initially allotted, we would be able to cover all the mandates of HAVA.

Mr. LARSON. What about the commingling of funds? Is this a temptation of States to use—you are smiling, so I take it—

Ms. ROGERS. I read the same article that you did. In Georgia, our State legislature okayed \$54 million in bond funding prior to HAVA ever being enacted. We reimbursed—when we got this last bit of money, we reimbursed our State Treasury. Now they are going to use that money, I assume they are going to use that money to pay down the bond debt. But a great deal of that bond debt had already been paid. It leaves a chunk of money that the Treasury then has.

I believe what you read may have been how the State is going to use the reimbursement once they already pay the bond funding.

Ms. LAVINE. I work on the county level so I am not sure how much the State would need. We also—in California we were able to pass a voter bond that allowed us to have some money in our county and throughout the State. So we have been fortunate that

we have got—I don't want to say enough money—but we probably have more than some of the other States have.

Mr. LARSON. Pretty much unanimous consent amongst the three of you that if we were to put technologically a draft on the DREs' paper trail, that that is realistically not something that would—that is going to fulfill the mission come this election in November; is that fair to say?

Ms. ROGERS. In Georgia we have determined that it would cost us \$16 million to retrofit our equipment for the addition of a paper trail to do that statewide. We don't think that is a good use of our HAVA dollars. And we don't have \$16 million of HAVA money left at this point to do so.

Mr. LARSON. I seem to garner from your testimony that you thought that the problems that were raised—not the least of which is the potential for the machine clogging, people reviewing, the time that could be allotted, people just walking away because that is what they are used to after they cast their vote because they have got to get back to work or whatever—becomes more problematic. Is that a fair assessment to say?

Ms. ROGERS. I think so.

Mr. LARSON. What about the decertification issue?

Ms. LAVINE. Because of the decertification, since Sacramento County did not have a DRE in March, we are not allowed to even purchase one in December. We are going to go to an optical-scan system for November. With all the legislation that is being passed, until there is a system with a paper, accessible voter-verified paper audit trail, we are not even allowed to purchase one.

Mr. LARSON. You may have heard Dr. Rubin's testimony earlier where he seemed to come up with a process that was different than the ones that you have testified to. And again, I am not a scientist. I am not someone who—what Professor Negroponte used to call one of the digitally homeless in many respects. So I don't want to mischance what he said. But it seemed to me he had a more compact and precise way of using that, though I think he testified that that is something that wouldn't be ready for this election cycle. I am wondering if you heard that and what your reaction might be long term with respect to the—at the heart of this argument, it is hard to deny when I face groups and they say, Well, what is the matter with trust but verify, or trust everyone but cut the cards, and being able to have that, know that you voted for that. And of course, it is a very logical assumption until you meet—come face to face with the practicality of its implementation and then all the ensuing fallout that has been mentioned, whether it is the disability community or others.

Mr. Shamos testified that he thought there would be a way to do that down the road, but it doesn't seem as though—clearly, it is not possible for November. But what is your sense about where we need to go for the future, and are these practical ways?

Ms. ROGERS. Well, let me first address what I heard Dr. Rubin talk about in that—you would. Instead of seeing that paper receipt, there is a possibility of printing it out. It probably would be an 18-inch-long ballot. These are just concepts. No one has developed anything like this. It might have like, if you voted on an optical scan, an 18-inch piece of paper. I have seen a prototype where this

would come up at the same time you are viewing your ballot on an electronic machine, and then you would look at it, as you looked at this side, you look at this side, and once you verify it, you would hit print and it might print out on card-stock paper. Understand that card-stock paper that you are currently printing an optical-scan ballot on goes for about \$0.35 a piece. Each voter would have this card-stock paper. It would come out. They would verify it and then they would take it to an optical-scan tabulator and vote, putting it into the tabulator, which gets back into the same scenario we talked about a little while ago. You have one of those per every precinct, versus having one voting booth with electronic capability for each voter. That in itself is two separate voting systems with two separate problems.

And what I have heard knocked around is these need to be from different vendors as well. You may not want them to be the same vendor. You have to get two vendors to work together for their software to integrate together, and there is a lot of proprietary concerns over that. But the biggest problem, one I don't think this money is growing on trees, and that is a whole lot of money.

Mr. LARSON. Do you ever feel that when all of these proposals are being made, that maybe what we ought to do is convene you all first?

Ms. ROGERS. We would appreciate that.

Mr. LARSON. My final question has to deal with this New York Times article that I think makes an awful lot of sense.

[The information follows:]

*The New York Times***The Disability Lobby and Voting**

11 June 2004

Two obvious requirements for a fair election are that voters should have complete confidence about their ballots' being counted accurately and that everyone, including the disabled, should have access to the polls. It is hard to imagine advocates for those two goals fighting, but lately that seems to be what's happening.

The issue is whether **electronic voting machines** should provide a "paper trail" -- receipts that could be checked by voters and used in recounts. There has been a rising demand around the country for this critical safeguard, but the move to provide paper trails is being fought by a handful of influential advocates for the disabled, who complain that requiring verifiable paper records will slow the adoption of accessible **electronic voting machines**.

The National Federation of the Blind, for instance, has been championing controversial voting machines that do not provide a paper trail. It has attested not only to the machines' accessibility, but also to their security and accuracy -- neither of which is within the federation's areas of expertise. What's even more troubling is that the group has accepted a \$1 million gift for a new training institute from Diebold, the machines' manufacturer, which put the testimonial on its Web site. The federation stands by its "complete confidence" in Diebold even though several recent studies have raised serious doubts about the company, and California has banned more than 14,000 Diebold machines from being used this November because of doubts about their reliability.

Disability-rights groups have had an outsized influence on the debate despite their general lack of background on security issues. The League of Women Voters has been a leading opponent of voter-verifiable paper trails, much to the dismay of many of its members, in part because it has accepted the disability groups' arguments.

Last year, the American Association of People With Disabilities gave its Justice for All award to Senator Christopher Dodd, an author of the Help America Vote Act, a post-2000 election reform law. Mr. Dodd, who has actively opposed paper trails, then appointed Jim Dickson, an association official, to the Board of Advisors of the Election Assistance Commission, where he will be in a good position to oppose paper trails at the federal level. In California, a group of disabled voters recently sued to undo the secretary of state's order decertifying the **electronic voting machines** that his office had found to be unreliable.

Some supporters of voter-verifiable paper trails question whether disability-rights groups have gotten too close to voting machine manufacturers. Besides the

donation by Diebold to the National Federation of the Blind, there have been other gifts. According to Mr. Dickson, the American Association of People with Disabilities has received \$26,000 from voting machine companies this year.

The real issue, though, is that disability-rights groups have been clouding the voting machine debate by suggesting that the nation must choose between accessible voting and verifiable voting.

It is well within the realm of technology to produce machines that meet both needs. Meanwhile, it would be a grave mistake for election officials to rush to spend millions of dollars on paperless **electronic voting machines** that may quickly become obsolete.

Disabled people have historically faced great obstacles at the polls, and disability-rights groups are right to work zealously for accessible voting. But they should not overlook the fact that the disabled, like all Americans, also have an interest in ensuring that their elections are not stolen.

Making Votes Count: Editorials in this series remain online at nytimes.com/makingvotescount.

MAKING VOTES COUNT

Document NYTF000020040611e06b0002k

New York Times

June 13, 2004

MAKING VOTES COUNT

Gambling on Voting

If election officials want to convince voters that electronic voting can be trusted, they should be willing to make it at least as secure as slot machines. To appreciate how poor the oversight on voting systems is, it's useful to look at the way Nevada systematically ensures that electronic gambling machines in Las Vegas operate honestly and accurately. Electronic voting, by comparison, is rife with lax procedures, security risks and conflicts of interest.

On a trip last week to the Nevada Gaming Control Board laboratory, in a state office building off the Las Vegas Strip, we found testing and enforcement mechanisms that go far beyond what is required for electronic voting. Among the ways gamblers are more protected than voters:

1. The state has access to all gambling software. The Gaming Control Board has copies on file of every piece of gambling device software currently being used, and an archive going back years. It is illegal for casinos to use software not on file. Electronic voting machine makers, by contrast, say their software is a trade secret, and have resisted sharing it with the states that buy their machines.
2. The software on gambling machines is constantly being spot-checked. Board inspectors show up unannounced at casinos with devices that let them compare the computer chip in a slot machine to the one on file. If there is a discrepancy, the machine is shut down, and investigated. This sort of spot-checking is not required for electronic voting. A surreptitious software change on a voting machine would be far less likely to be detected.
3. There are meticulous, constantly updated standards for gambling machines. When we arrived at the Gaming Control Board lab, a man was firing a stun gun at a slot machine. The machine must work when subjected to a 20,000-volt shock, one of an array of rules intended to cover anything that can possibly go wrong. Nevada adopted new standards in May 2003, but to keep pace with fast-changing technology, it is adding new ones this month.

Voting machine standards are out of date and inadequate. Machines are still tested with standards from 2002 that have gaping security holes. Nevertheless, election officials have rushed to spend hundreds of millions of dollars to buy them.
4. Manufacturers are intensively scrutinized before they are licensed to sell gambling software or hardware. A company that wants to make slot machines must submit to a

background check of six months or more, similar to the kind done on casino operators. It must register its employees with the Gaming Control Board, which investigates their backgrounds and criminal records.

When it comes to voting machine manufacturers, all a company needs to do to enter the field is persuade an election official to buy its equipment. There is no way for voters to know that the software on their machines was not written by programmers with fraud convictions, or close ties to political parties or candidates.

5. The lab that certifies gambling equipment has an arms-length relationship with the manufac-

turers it polices, and is open to inquiries from the public. The Nevada Gaming Control Board lab is a state agency, whose employees are paid by the taxpayers. The fees the lab takes in go to the state's general fund. It invites members of the public who have questions about its work to call or e-mail.

The federal labs that certify voting equipment are profit-making companies. They are chosen and paid by voting machine companies, a glaring conflict of interest. The voters and their elected representatives have no way of knowing how the testing is done, or that the manufacturers are not applying undue pressure to have flawed equipment approved. Wyle Laboratories, one of the largest testers of voting machines, does not answer questions about its voting machine work.

6. When there is a dispute about a machine, a gambler has a right to an immediate investigation. When a gambler believes a slot machine has cheated him, the casino is required to contact the Gaming Control Board, which has investigators on call around the clock. Investigators can open up machines to inspect their internal workings, and their records of recent gambling outcomes. If voters believe a voting machine has manipulated their votes, in most cases their only recourse is to call a board of elections number, which may well be busy, to lodge a complaint that may or may not be investigated.

Election officials say their electronic voting systems are the very best. But the truth is, gamblers are getting the best technology, and voters are being given systems that are cheap and untrustworthy by comparison. There are many questions yet to be resolved about electronic voting, but one thing is clear: a vote for president should be at least as secure as a 25-cent bet in Las Vegas.

Re "The Disability Lobby and Voting" (lead editorial, June 11):

The American Association of People with Disabilities (AAPD) strongly supports election systems that are accessible, verifiable and secure. We oppose the "paper trail" requirements that have been proposed by California and others because we are not convinced that a voter-verified paper ballot will in fact make elections more secure, and we know that these requirements violate federal accessibility mandates.

Accessible touchscreen voting has already been implemented in states like Maryland and Georgia in a manner that has improved the accuracy and security of elections.

We also know that state requirements of paper trails, at least for now, are creating access problems for voters with some types of disabilities, and are delaying accessibility for people with limited English proficiency.

The editorial asserted that the League of Women Voters has been a leading opponent of paper trails "in part because it has accepted" the arguments of AAPD and other disability groups. In fact, AAPD has followed the League's lead on this issue because we respect its long history and expertise in advocating for fair and accurate elections.

The editorial correctly reported that AAPD has received a total of \$26,000 from voting machine companies this year. Our 2004 budget, which exceeds \$2 million, includes contributions from a wide variety of sources.

We advocate for policies that are in the best interests of all people with disabilities, and do not let any funding source threaten our independence and integrity. For example, we received more than \$100,000 from pharmaceutical companies this year, but we opposed the Medicare prescription drug legislation that was recently enacted with strong support from that industry.

AAPD worked closely with Senators Mitch McConnell and Christopher Dodd and Representatives Bob Ney and Steny Hoyer on the accessibility requirements in the Help America Vote Act (HAVA) of 2002. Because of this important legislation, America has the potential to realize dramatic improvements in election accessibility and accuracy. AAPD will continue to advocate for election systems that can accomplish these equally important goals.

Sincerely,

Andrew J. Imparato
President and CEO
American Association of People with Disabilities (AAPD)
1629 K Street, NW, Suite 503
Washington, DC 20006
800-840-8844 (V/TTY); 202-457-0473 (FAX)
visit our website: www.aapd-dc.org

Mr. LARSON. You heard Dr. Shamos refer to it. The article, though you may not have read it, essentially said we ought to make sure when it comes to voting that we are going procedurally from a security standpoint and from testing, et cetera, that we provide the voters with the same kind of security that is provided in the casino industry for the integrity of slot machines. We ought to make sure that the security is there as well.

I am gathering from your testimony that you wouldn't disagree with that but what you need for that is the money in the independent verification. Is that fair to say?

Ms. LAMONE. And we need—for the country to be comfortable, we need to have standards that everybody must follow and we need to have somebody looking at the software, like I mentioned before, in establishing a baseline for the security issues, telling the States what risks were identified and maybe how to mitigate them, just like we did in Maryland with those two reports.

Last year it was just a fun-filled year with all the security reports coming out. Election officials don't have that expertise. We know how to run an election but we are not security experts, which is why I now have security people on my staff. And then you would have some assurance that the country using X vendor system is all addressing the same issues and hopefully around the same ways.

Mr. LARSON. You would agree with Mr. Rubin that they should be independently evaluated also, not evaluated by the vendors themselves?

Ms. LAMONE. No, no. I think NIST is an appropriate vehicle. And I for one am so glad HAVA was enacted and glad that NIST is involved in the process, because it does provide us with a lot of weapons that we never had before.

Mr. LARSON. I want to thank you all. I think you have been terrific. And I thank the Chairman again for his leadership on this important issue. He rarely takes the bows that he richly deserves, but he has been a leader in this area in passing what I believe is historic and landmark legislation; like all legislation, not ones that we can't further perfect as we go along, but given the circumstances and the times and trying to put this in order and having to buck a trend, he deserves an enormous amount of credit. And thank you for providing these hearings and providing people with the opportunity to voice their concerns so we can better implement the laws of HAVA.

The CHAIRMAN. Thank you. I want to thank my cousin in the back of the room applauding for me. I want to thank you. And I want to thank all the people across the country that worked on this and gave the input to get HAVA to where it is today. I thank our witnesses who worked hard to prepare for the hearing. We had two great panels.

I thank Congressman Larson for his diligence and his staff, and the members and other members of the committee and their staffs, for their work on this.

I ask unanimous consent that members and witnesses have 7 legislative days to submit material into the record, and those statements and materials be entered in the appropriate place in the record. Without objection, the material will be entered.

I ask unanimous consent that staff be authorized to make technical and conforming changes on all matters considered by the committee today. Without objection, so ordered.

And, having completed our business, the hearing is adjourned.
[Whereupon, at 2:15 p.m., the committee was adjourned.]

Chairman Ney's Response to the New York Time Editorial of June 11, 2004

In a recent editorial ("The Disability Lobby and Voting," Jun. 11, 2004), the New York Times disgraced itself by making slanderous attacks against representatives of the disability community who have opposed legislation that would require electronic voting systems to produce a voter-verified "paper trail." The editorial states that this opposition, which the New York Times believes is disproportionately influential, is most likely due to contributions that groups like the National Federation of the Blind (NFB) and the American Association of People with Disabilities (AAPD) have received from voting equipment manufacturers. In other words, the New York Times is more or less alleging that the representatives of these groups are selling out their own constituents as well as the American electorate in exchange for a pay-off.

This is simply outrageous. As a principal author of the Help America Vote Act of 2002 (HAVA), I had the opportunity to work closely with both NFB and AAPD as this legislation was being developed. Thus, I know from first-hand experience of their commitment to improving the election process not only for those they directly represent but for all Americans as well. Their input added greatly to a landmark piece of legislation that will substantially improve our nation's voting system for generations to come.

People of good will have honest disagreements about the advisability of requiring electronic voting systems to produce voter-verified paper records. Groups like NFB and AAPD, as well as many other respectable voices in the technology and election administration communities, have legitimate concerns about whether such a requirement would compromise the privacy and independence of voters, add unnecessary expense to the process, and do nothing to buttress the integrity of the election system.

Unfortunately, the New York Times refuses to even acknowledge that reasonable opponents of a paper-trail requirement even exist. Instead, it implies that only those who have corrupt motives or have been bought off could possibly oppose such a requirement.

The editorial also smears my good friend, Senator CHRISTOPHER DODD, by implying that there is something untoward about him appointing Jim Dickson, head of AAPD, to the Advisory Board of the Election Assistance Commission after the AAPD had awarded the Senator with its Justice for All Award. This perception of a conspiracy around every corner is beginning to descend into the paranoid depths occupied by Oliver Stone and Michael Moore. This is unbecoming of an institution as venerable as the New York Times, and the American public deserves better.

The whole issue of electronic voting system security is extremely important and very complex, and the committee I chair will continue to examine it closely. Thus, there is a need for a healthy de-

bate on this issue. However, that debate is impoverished when a voice of prominent as the New York Times' slurs opponents of its positions with outlandish speculation and unfounded charges. What is needed is more reasoned dialogue and less character assassination.

