Mr. PUTNAM. We are going to do a 5-minute round of questions, get through everyone, and then do another round if we so desire. Considering the number of committee members who are here, I think we will certainly have time to do that.

Technology changes rapidly. Obviously local governments don't have the luxury of changing election systems with every cycle, but a number of these new systems are new. I mean, they are new concepts, they are new approaches.

Mr. Hite, if you would, evaluate these newer models, optical scan and the DREs, for us and rank them in terms of accuracy, security and access for those who traditionally have not had good access to the ballot.

Mr. HITE. I would be happy to, but I would like to preface it with addressing the question on two levels. You can talk about the types of equipment in general, but it really also requires getting down to specific make and model, because while DREs, for example, commonly offer certain features with respect to accuracy or with respect to security, how they are actually implemented in the system, and then how they are actually implemented within the jurisdiction, will determine how well they perform.

So, with that preface, I will make a couple of comments based on our 2001 work, where we surveyed vendors and we surveyed jurisdictions with respect to these characteristics of performance. As a general rule, when it came to ease of use and efficiency, how quickly they can capture and count, and the costs associated with doing that, DREs generally had a higher rating than the other types of voting equipment. With regard to security based on features, notwithstanding how they have been implemented, that with regard to security, DREs and optical scan were roughly the same. And then with regard to accuracy across all types of equipment, whether it is jurisdictions or vendors, they basically viewed the accuracy of the systems to be somewhat the same.

Now, I would add another qualification with that with regard to the jurisdictions, and that is when we followed up with certain jurisdictions to see what data are actually collected and are behind these impressions, we learned that is exactly what they are, they are impressions or viewpoints on performance.

The data are pretty sparse in terms of what are collected relative to the performance of any of the types of systems, which is one of the long-term challenges that we have laid out that needs to be addressed. If we are going to make strategic, long-term, informed decisions about what kind of technology to use, you have to base it on some good data, and in terms of a performance standpoint out there across the jurisdictions, that data basically are not being captured.

Mr. PUTNAM. Dr. Semerjian, do you want to field that as well?

Dr. SEMERJIAN. Well, I basically agree with the comments made by Mr. Hite. I think the DREs can improve their performance with the appropriate standards and testing protocols. I think that is really where we still have a perception that these systems are not tested properly. We don't have national standards; implementation is varied from State to State, from precinct to precinct. I think with the proper establishment of proper standards and testing procedures, I think DREs can improve our ability to provide secure, pri-

vate voting ability and accuracy. And also, I think it was pointed out by Mr. Hite, it can improve in terms of enabling voters with disabilities. That's something that perhaps the other systems do not. I think that is something we need to keep in mind.

Mr. PUTNAM. Mr. Jarrett, how many different voting systems are employed throughout Missouri?

Mr. JARRETT. In Missouri we have three types. We do some counties that still operate under the paper ballot system. We have punch card systems and also optical scan systems.

Mr. PUTNAM. And the decision on which type to deploy is made by whom?

Mr. JARRETT. That is made by the local election officials in every county.

Mr. PUTNAM. And how many of those are there? How many different counties do you have?

Mr. JARRETT. We have 116 election authorities. The urban areas such as St. Louis, Kansas City, St. Louis County and Jackson County have boards of election commissioners that are appointed by the Governor, and they run elections in those areas. The rest are run by county clerks.

Mr. PUTNAM. Has there been a high turnover since 2000?

Mr. JARRETT. Of county clerks?

Mr. PUTNAM. No, of technology.

Mr. JARRETT. Oh, I'm sorry.

Mr. PUTNAM. Changes in the method of electioneering.

Mr. JARRETT. Well, Missouri is the ShowMe State, so we have been sort of taking a wait-and-see attitude.

Mr. PUTNAM. Wait on Florida to show you the way, right?

Mr. JARRETT. Yes, that's right. We have had eight counties that moved from the punch card to the optical scan for this election. Several of the counties are waiting, looking at the DREs very closely, and, of course, some of the counties that had optical scan had the central count, and they are moving toward the precinct counters, so not much turnover. Again, we are sort of adopting the wait-and-see approach.

Mr. PUTNAM. My time expired. I will yield to Mr. Clay also. Boy, 5 minutes goes by pretty fast.

Mr. CLAY. Yes, it does. You were having fun, Mr. Chairman.

Mr. Hite, in your testimony you communicate that certain voting machines pose a certain risk. Do you have a certain set of recommendations for local election officials to minimize those risks?

Mr. HITE. The short answer is no, sir, I don't have a set of recommendations handy for those jurisdictions. I would observe, however, that this is one of the things that the Election Assistance Commission was set up to do, and I believe they are on brink of releasing best practices for the local jurisdictions to employ in the 2004 elections.

Mr. CLAY. You know, the Election Assistance Commission has a budget of $1.5 million for fiscal year 2004. Is that adequate for them to meet their obligations for the 2004 elections?

Mr. HITE. I know, in talking to the Commission Commissioners, that they do not believe that it is adequate, and I believe they are in the best position to make a judgment as to whether or not it is adequate or not. I know under HAVA they were authorized up to

$10 million a year, and I would only submit, from my viewpoint, that their role in this, as is the role of NIST, is extremely important and worthy of adequate funding to ensure that they can do what they were set up to do under HAVA.

Mr. CLAY. Does certification guarantee that the software is free of malicious code, and, if so, how is that accomplished?

Mr. HITE. No sir, the answer to your question is no, it does not guarantee that. There is no system that offers a guarantee of that.

Mr. CLAY. Does it guarantee that the machine cannot be tampered with during the election?

Mr. HITE. No sir.

Mr. CLAY. No. OK. Thank you for your responses.

Dr. Semerjian, it is my understanding that the work at NIST on standards for computerized voting machines was halted this year because of a lack of funding; is that correct?

Dr. SEMERJIAN. Well, things slowed down, let's say, but, in fact, let me make it clear that the standards are not going to be set by NIST. They will be set eventually by TGDC. So TGDC just got started. So we have done, as I pointed out, some of the background work on human factors and on security issues, but as far as setting standards and guidelines, TGDC had to do that, which did not get going until 2 weeks ago.

Mr. CLAY. Let me ask you, what was your budget request for election work for 2004, and what will be your request for 2005?

Dr. SEMERJIAN. There was no request in the 2004 budget. For 2005, the EAC has requested a budget of $10 million for NIST, not for 1 year, but basically for the entire work to be done, which will probably be done over a 3-year period. But I think if that $10 million is provided, we feel that is adequate funding for NIST to get the job done.

Mr. CLAY. OK. NIST has a responsibility under the Help America Vote Act with regard to the development of technical standards for voting systems. When do you think these standards will be ready? And I heard you say in your testimony you have had the initial meeting?

Dr. SEMERJIAN. Right. Basically HAVA legislation requires us to make the first set of recommendations within 9 months after the formation of TGDC. So the clock just started running.

Mr. CLAY. OK. Thank you for those answers.

Mr. CLAY. Mr. Jarrett, the Secretary of State in Missouri has declared that no electronic voting machines will be used in Missouri that do not provide a voter verification paper trail. Has any electronic voting equipment been certified for use in Missouri, and, if so, will any be used in the St. Louis area?

Mr. JARRETT. The answer to that is no, none have been certified. In Missouri, State statute requires that before the Secretary of State can certify equipment for use in Missouri, that it has to be certified to the current standards by an independent testing authority. And as of this date, no vendor has submitted that ITA certification to the Secretary of State, so there will be none used in Missouri this year.

Mr. CLAY. During the debate at the Election Assistance Commission hearing in May, there was a concerned voice by the disability community that computerized voting machines with verified paper

ballots would be a step backward for the visually impaired. In research done by your office, how have you addressed that problem?

Mr. JARRETT. Well, we have looked at, of course, that's a very serious problem, and it is one that I know Secretary Blunt takes very seriously. We have looked at a written opinion from the Department of Justice on that issue that talks about DREs that produce paper ballots; as long as they produce a similar experience for disabled voters, that it complies with HAVA and the Americans with Disabilities Act. And in Missouri, Secretary Blunt has appointed a committee, an equipment certification committee, where we have a representative from a disability advocacy group that's a member, and we also have two members from the blind community that are on the committee. And they have been very helpful in educating the rest of the committee on the disability issues, and they will certainly be very important in certifying. And Secretary Blunt will consider their input before he certifies equipment to make sure that it is accessible to the disabled.

Mr. CLAY. Thank you for your answer.

My time is up, Mr. Chairman.

Mr. PUTNAM. Mr. Holt.

Mr. HOLT. Thank you very much, Mr. Chairman, and I appreciate the opportunity to join you here, and I certainly like the Florida orange juice. That's a nice touch. We all extol the contributions of Florida in the orange juice field.

Mr. PUTNAM. We have to have something positive to say about Florida this morning.

Mr. HOLT. Well, indeed, in 2000, we all got an education. Americans got an education in voting. Many of us who had been involved in the business knew it is complex. As one who won a reelection by less than 1 vote per precinct, I certainly had paid attention to the mechanisms and as well as the technology of voting.

But for most Americans, it was previously thought to be very simple, and I think we have all learned a lot. I think we have learned that we have to hold up the principles that voting will be fair, that it will be accessible, and that it will be verifiable, and it is that latter principle that I wanted to talk about today.

I noticed your hearing calls for technology, accuracy, reliability and security. I would add another, auditability or verifiability, as what we should be looking at today.

And my first question, actually, I guess, is probably for Mr. Hite and for Mr. Semerjian. Considering that it is a secret ballot, is it possible for anyone other than the voter, be it the manufacturer, vendor or election official—is it possible for anyone other than a voter to verify whether the voter's intentions have been appropriately recorded?

Mr. HITE. I have never pondered that question before, so that is why I pause.

Mr. HOLT. I think it is the fundamental question here.

Mr. HITE. My quick response to that is I don't think it is possible for anyone other than the voter to know the voter's intent and be able to verify the voter's intent. You would have to require some element of the voter's interaction to do that.

Mr. HOLT. Dr. Semerjian.

Dr. SEMERJIAN. Well, let me perhaps answer a different and related question.

Mr. HOLT. OK.

Dr. SEMERJIAN. That is the fact that the paper ballot is verified does not necessarily mean that the computer-recorded vote is verified. I mean, they are related, but they are two different things. So I think we need to make sure that we should not be satisfied simply by saying the paper ballot, the paper ballot is the intent of the voters.

We need to make sure that the computer-recorded vote records properly the intent of the voter, and I think that's done through a proper testing, through providing proper security and data integrity measures.

Mr. HOLT. Well, let me follow on that point, Mr. Semerjian. In your testimony you talk about performance-based standards. I take that to mean you like to look at the outcome in an applied way, where it is actually used in the field, to see whether the result is correct, rather than relying on procedures that the room is locked, and that no one else has access to the software or whatever training and procedural steps one takes. So, given that, with performance-based standards, how can you know whether a machine has an error in it, perhaps in a software, perhaps unintentional, perhaps hacked? How can you know that on a performance basis?

Dr. SEMERJIAN. Well, that's normally done by subjecting the equipment that is being tested to certain inputs. Statistically——

Mr. HOLT. But that's beforehand. That's not performance-based. As I understand what you mean by performance-based standards, you want to know whether, as it is used in the field, whether the numbers match up with some independent measurement.

Dr. SEMERJIAN. The idea of the performance-based standard is not to simply say you have to do this and that and the other thing, but to simply say, OK, if applied, if I use that equipment the way it is supposed to be used. Then does the machine, at the end, produce the exact input as an output? That's really what is meant by performance standard—and with what level of accuracy? I mean, is there a discrepancy at the 1 percent level, or what is our expectation; is 1 percent acceptable, or 5 percent?

Those are the kinds of standards we can accept, not telling vendors that you have to do this, you have to save the data this way, etc. I think we want to leave the creativity, the innovation part to the vendor, but require them to deliver an equipment, the machine, that provides 100 percent accurate performance.

Mr. HOLT. Well, the time is up. I am not sure I got an answer to how do you know whether the machine has been hacked or not, but time has expired, so thank you.

Thank you, Mr. Chairman.

Mr. PUTNAM. Thank you.

Mr. Hite or Dr. Semerjian, do you know how many individual election units there are in this country, how many precincts there are in this country?

Mr. HITE. The numbers I have seen on the precincts, are on the order of 193,000.

Mr. PUTNAM. 193,000 precincts, and presumably some of them in very rural areas might just have one or two machines, and another might have a couple of dozen?

Mr. HITE. I was speaking to precincts, polling places, in terms of jurisdictions, voting jurisdictions, there's only on the order of 10,000. Each of these precincts have multiple polling places associated with them.

Mr. PUTNAM. So there are 193,000 polling places?

Mr. HITE. Correct, where you go to vote, the local school, church.

Mr. PUTNAM. Right. Each of which may have one or two machines or private little areas where you go do your paper ballot, pull the paper ballot or lever or whichever it may be, up to a dozen at each precinct, something like that.

Mr. HITE. Configurations go by equipment and size.

Mr. PUTNAM. But we are talking about a lot?

Mr. HITE. Yes.

Mr. PUTNAM. It could be several hundred thousand starting at a baseline of almost 200,000?

Mr. HITE. Yes.

Mr. PUTNAM. So, let me just say something about Florida, because I think it is important. Anyone could have been Florida in 2000, and, in my opinion, we haven't passed any regulation that will prevent another Florida in 2004. Nothing we have done, nothing we will talk about, nothing we can do will prevent a close election, which is really what happened.

I mean, when you talk about what happened in Florida, you had a close election, and it was not the first time that it had happened. Even in my short time, county commissioners have been elected and then unelected because the outcome of a vote turned by five votes or three votes, because there were human beings involved and somebody forgot to—the deputy who delivered the boxes of ballots to the central accounts location thought he had unloaded all the ballots and found another box in his car the next morning, or the very well-meaning, well-trained coworkers just picked up three paper ballots, and they thought they only had one, fed it into the machine, and so the top one was red, the bottom two were not.

When you get down to several hundred thousand machines counting millions of votes, there will be errors, because humans are involved. So let me just ask what the HAVA act will do to prevent the same errors, the same oversights, the same mistakes that were made in 2000. What has changed as a result of that legislation?

Mr. HITE. I don't believe that the HAVA act will fundamentally change that for the 2004 election. The HAVA act has in it provisions for long-term improvement in this area, as well as short-term, because steps have already been taken by the EAC in a relatively short amount of time to recognize and inform and educate the jurisdictions about where improvements can be made in the near term to minimize the chance of those errors. We are never going to get rid of them. That's what we are trying to do is minimize them. And whether similar problems will surface in 2004, I would be shocked if they didn't, and particularly because the whole election process is going to be under such a microscope now and going forward. But what we are talking about, what HAVA does,

and what we are talking about doing near term and long term, is to reduce the probabilities of this happening.

Mr. PUTNAM. Is there a margin of error in every voting process and voting technology that is deployed today?

Mr. HITE. There is a margin of error in every process involved in any type of business or government activity, including air traffic control, for example, where you want accuracy down to five nines, so it is inevitable.

Mr. PUTNAM. Over the long term, is a paper trail the way to go? Is a paper trail the best, most effective way to audit the results of an election?

Mr. HITE. I believe a paper trail can offer a layer of security with respect to DREs. Now, it all depends on how you use that paper trail. Just having the paper receipt and having the voter look at it in and of itself doesn't give you a whole lot. But if you implement it in a way where you have some means to know whether or not the machine is capturing the vote as it is on the paper receipt, now you have added a level of security.

As with any decision about security capabilities, you have to make those decisions in the context of risk. What is the threat, what are my vulnerabilities, and how much am I willing to pay to reduce the risks associated with those two variables? And so you have to make decisions about that. You don't just throw money at something. You make good, fact-based decisions.

Mr. PUTNAM. And I would submit that time is also a factor, because it becomes a deterrent to voting, depending on how long it takes for all this verification to occur.

Dr. Semerjian, I want you to answer that question, and then we will yield to Mr. Clay.

Dr. SEMERJIAN. Well, I agree with what was said. I don't think I have anything to add. There is an uncertainty with every process. And the whole point is, how do you reduce that uncertainty to an acceptable level? So whether you expect 100 percent accuracy, which is almost unattainable, or whether 99.9 percent is acceptable or whether it is 95 percent, I think we certainly want to set standards that push that level, that level of certainty, or reduce the level of uncertainty as much as possible. And that can be done through proper testing and setting the proper standards to start with.

Mr. Chairman, may I answer, sir, the question that Mr. Holt asked that I could not answer?

Mr. PUTNAM. Sure.

Dr. SEMERJIAN. Regarding hacking, how do we know that it's hacked?

Mr. HOLT. Or error of any sort.

Dr. SEMERJIAN. Well, this is work in progress. As I said, TGDC had the first meeting. But one of the issues that they already addressed is this issue: How do we know that the software on a particular machine is not hacked or modified or changed by mistake? And we do have a National Software Reference Laboratory at NIST that we use for this kind of applications. We haven't used them for the voting process, but we have used it where at different stages of a process you can actually check the integrity or the signature of a particular software package, so that once you have established this referenced initial certified version of a software, you can check

against that at different stages so that there are no mistakes made in duplication, or, changes by mistake, so that you can verify the integrity of that software from the very beginning of the process to the very end where it is loaded to individual machines.

So we haven't worked out all the details, but I think that the technology is there to be able to say that this particular software package is not what it was at the beginning of the process, that something has changed, and alert the officials that some action needs to be taken.

Mr. PUTNAM. Mr. Holt, how about if I just go ahead and recognize you for your second wave of questions?

Mr. HOLT. Well, just following on that point. In fact, that is right; the way you test software is you see whether it gives the right answer. In other words, you audit it. You compare it against another approach to that same calculation to see if it gives the same result. And you do that at each stage along the way. You also check the software to see whether it is robust in various ways.

Dr. SEMERJIAN. May I say something?

Mr. HOLT. Yes.

Dr. SEMERJIAN. This is not only substantiating the result of the computation, because the program can give you the same result but in the meantime could produce some output of some other source. Here, the idea is to check the integrity of the entire software package.

Mr. HOLT. That is right. Step by step, you audit it.

Dr. SEMERJIAN. Well, it is more than that.

Mr. HOLT. And you compare each operation to see whether that operation does what you think it does.

Dr. SEMERJIAN. It is more than that. If any kind of a statement is changed in that software—which may still give the same answer—if any code is changed, the signature of the code will be changed. So even two codes that give the same answer may be slightly modified. And this kind of technology will detect that.

Mr. HOLT. That is external hacking. That might or might not find an embedded problem, an embedded bug that has been in there since it was written or since it left the package.

Dr. SEMERJIAN. That is where the certification process comes in.

Mr. HOLT. But, anyway, my point is the way you know anything, the way anything of value should be subject to audit—and my point is, if in fact the answer to my first question is that only the voter can verify his or her intentions are properly recorded, then the only audit that makes sense is to compare the result against what the voter has verified. But let me go on to a couple of other questions.

Mr. Hite, what do you think—you say in your testimony that we have to make sure that the people who work with these devices are well trained and have the requisite knowledge. What is the requisite knowledge to operate today's BREs? Is it more or less than the knowledge to maintain, say, keeping track of optical scan paper for the election workers?

Mr. HITE. What I can offer there as part of our survey of jurisdictions, in 2001 we asked local jurisdictions about whether or not DREs versus optical scans, etc., how difficult they were for operators, poll workers to use, or for voters to use, or how difficult it was to correct somebody's vote who made a mistake versus the different

types of technology. And in general, DREs were easier to operate than the optical scan and the other types of voting systems.

Specifically in terms of the training that is needed for a given poll worker, a given maintenance individual, anyone who has to interact with that system, that is going to vary by jurisdiction and by type of system because there's different rules and standards that govern how these elections are conducted—and we can use Missouri as an example of that.

Mr. HOLT. So if there are 50 million people this year who will be asked to vote on electronic machines, maybe 30 million will actually show up and vote. For those 30 million votes this year, what would you recommend is the best near-term solution to protect the integrity?

Mr. HITE. Coming from an organization where we don't make rash decisions or take or quick positions on things, I'd go back to what I said before. It requires a level of understanding and visibility into those systems—make and model of those systems—to know how they behave and know what their strengths and weaknesses are. I just don't have that because I haven't done that type of analysis on a system-by-system basis. And so my position would be that is the kind of decision that you want to make with the long-term focus in mind. You want to base it on some good data that talks about what are the vulnerabilities of those systems and what is the best way to implement paper receipts if you choose to do that. I am just not in a position to give you the answer that you are looking for. I don't have that kind of knowledge.

Mr. HOLT. And with my time expired, I just want to thank the Show Me State and Secretary Blunt for his, I think, intelligent approach to this and his leadership.

And thank you, Mr. Chairman.

Mr. PUTNAM. Mr. Clay.

Mr. CLAY. Thank you, Mr. Chairman.

Mr. PUTNAM. And I will note for the record the presence of the gentlelady from Ohio, Ms. Kaptur. Without objection, you are certainly welcome to join us, and we are delighted to have you here and certainly hope that should you wield the gavel in your appropriations subcommittee, that I will be accorded the same treatment when you all are——

Ms. KAPTUR. Yes.

Mr. PUTNAM. Thank you.

Mr. Clay.

Mr. CLAY. Thank you.

Mr. Hite, the California Secretary of State has established a set of safety criteria that, if met by election officials, will allow the recertification of the computerized voting machines. Would you comment on the adequacy of those recommendations?

Mr. HITE. Yes, sir. I am aware, as you say, that there are these 23 conditions. I am not, unfortunately, familiar with those 23 conditions so that I can offer an informed opinion on it. So I apologize for that.

Mr. CLAY. In your full written testimony, you state that current touch-screen electronic voting machines can produce images that can be printed, but explain that this is according to vendors. Did

GAO investigate whether the machines currently in use do in fact have this potential?

Mr. HITE. No sir, we did not. We have done no code reviews or any testing or evaluation of specific make and models to determine what features are implemented and whether or not they have been implemented properly. I believe that other witnesses at this hearing have much more in-depth knowledge about the specific make and models.

Mr. CLAY. Thank you.

Dr. Semerjian, when the new standards are ready, what do you suggest that States do if they have already purchased voting machines with HAVA funds and then find out that the new machines are not HAVA compliant? What should they do?

Dr. SEMERJIAN. I am not quite sure how to answer that question.

Mr. CLAY. I want to hear your answer.

Dr. SEMERJIAN. I think this is exactly the issue they are struggling with. They feel that they are between a rock and a hard place, because they need to make some changes perhaps, and yet the information that they need to make informed decisions regarding purchases is not available. So, I mean, I really feel for them, but unfortunately the timing was such that these standards could not be provided in time certainly to affect this year's elections, but we hope that they will be for the 2006 elections.

Mr. CLAY. So some States got ahead of everyone else because of HAVA, and now that may come back to bite them?

Dr. SEMERJIAN. Well, I mean, this is strictly conjecture on my part. But I mean, it sort of depends on what the changes needed will be. I mean, if there are software changes, they certainly can be made relatively inexpensively. But if there are going to be major hardware changes, obviously they will be more costly.

Mr. CLAY. Let me also ask, whose job is it to assure that electronic voting machines are free of malicious code and actually register the votes as intended? Whose job would that be?

Dr. SEMERJIAN. Elections are run, to the best of my knowledge, by local officials. So it is their responsibility to ensure the integrity of the voting process. The EAC, TGDC, and other organizations try to provide them with the information, knowledge, and the tools, technology tools to make that job as tenable as possible. But at the end of the day, it is the local officials' responsibility to ensure the integrity of the voting process.

Mr. CLAY. Thank you for those responses.

Mr. Jarrett, it is my understanding that none of the touch-screen machines now on the market have been certified to the 2002 standards. Is that correct?

Mr. JARRETT. That is my understanding as well.

Mr. CLAY. Did the lack of certification play a role in the Missouri Secretary of State's decision to defer the use of computerized voting machines in Missouri?

Mr. JARRETT. Yes. Again, our State statute requires that anytime that the Secretary of State certifies equipment, it has to be certified by an ITA to the current standards, which are the FEC 2002 standards currently, d will be the EAC standards when the Standards Board and the TGDC sets those standards. So, yes, it played the major role, as a matter of fact.

Mr. CLAY. I thank you for your response and the entire panel being here.

Mr. Chairman, I yield back the balance of my time.

Mr. PUTNAM. Thank you, sir.

Ms. Kaptur.

Ms. KAPTUR. Yes, Mr. Chairman. Thank you so much for allowing us to participate in your important hearing this morning and also for the Florida orange juice. I now had that for breakfast and for lunch, and appreciate the work that the people of your State do for the rest of the world.

Thank you very much. And I wanted to thank the witnesses for producing this excellent report this morning. This is a topic on which we in Ohio are very, very focused, and appreciate your diligence.

I think more oversight is better than less oversight. I know that Congressman Clay in our conversations has been trying to receive information from those of us not on this subcommittee, not on this full committee, in the important area of voting technology and reform. And I just thought I would state for the record, and I will put the full information in the record, that in Ohio, about a year ago, five technologies that were being considered were displayed at our Statehouse in Columbus, OH. And at that time, not being a computer technology expert, I asked three of our major universities to select the best people they had, and they chose the people in charge of their computer security to go down and review the technologies on display. And I won't read you their full report, but I will read you some of the conclusions:

No technology currently under consideration had attributes that made it both secure and readily accessible for use. All of the technologies had serious shortcomings in these two major elements:

None of the security mechanism force of the voting systems that remained in consideration in Ohio could sufficiently prevent fraud or abuse.

The integrity of the voting process as well as voter confidence could be compromised through the absence of an auditible paper trail at each precinct. Without rigorous testing by multiple outside agencies with appropriate technical expertise, assurance of a secure era of tamper-proof electronic election system cannot be obtained. Levels of computer proficiency among the electorate vary and tend to disfavor the elderly, minorities, and the economically disadvantaged.

And we saw that in the election called the test election, which was held last year in which the technologies were employed.

And, finally, while electronic voting is a viable option that can be successfully implemented, it must use secure disciplines to gain the public's confidence.

After that information came to me, it got my attention, and particularly because our State was trying to get our local counties to purchase equipment and to sign contracts. And after my family and I voted in November, I sent a letter to our Secretary of State, November 10, 2003—and I am placing this in the record—to which I have received no response. But I would ask you if you are capable to answer any of these questions.