PUBLIC HEARING

STATE OF CALIFORNIA

SECRETARY OF STATE

SECRETARY OF STATE'S OFFICE

1500 11TH STREET

FIRST FLOOR AUDITORIUM

SACRAMENTO, CALIFORNIA

MONDAY, JULY 30, 2007

10:04 A.M.

JAMES F. PETERS, CSR, RPR
CERTIFIED SHORTHAND REPORTER
LICENSE NUMBER 10063

TIFFANY C. KRAFT, CSR, RPR
CERTIFIED SHORTHAND REPORTER
LICENSE NUMBER 12277

PETERS SHORTHAND REPORTING CORPORATION (916) 362-2345

APPEARANCES

SECRETARY OF STATE

Ms. Debra Bowen

PANEL MEMBERS

Mr. John Pérez, Moderator

Ms. Judith Carlson, Elections Divison Counsel

Mr. Lowell Finley, Deputy Secretary, Voting Systems Policies

Mr. Lee Kercher, Chief, Information Technology Division

Mr. Bruce McDannold, Interim Director, Office of Voting Systems Technology Assessment

Mr. Chris Reynolds, Deputy Secretary, HAVA Activities

ALSO PRESENT

Ms. Ana Acton, FREED

Ms. Kim Alexander, California Voter Foundation

Dr. Judy Alter, Protect California Ballots

Mr. Dan Ashby, Election Defense Alliance

Mr. Stephen Aye, Placer County

Ms. Ann Barnett, Kern County

Mr. Wayne Beckham, Riverside County ROV

Mr. Jerry Berkman

Ms. Judy Bertelsen, Alameda County

Mr. Matthew Bishop, University of California, Davis

Ms. Julie Bustamante, Lassen County Clerk-Recorder

APPEARANCES CONTINUED

ALSO PRESENT

Mr. Philip Chantri, Santa Clara County

Ms. Gloria Coutts, Placer County

Ms. Cathy Darling, Shasta County

Mr. Alan Dechert, Open Voting Consortium

Ms. Barbara Dunmore, Riverside County ROV

Ms. Teresa Favuzzi, California Foundation for Independent Living Centers

Mr. Dennis Floyd, San Diego County

Mr. Dero Forslund, Trinity County

Ms. Michelle Gabriel

Mr. Brett Garrett

Ms. Sharon Graham

Ms. Terry Hansen, Yuba County

Mr. Philip Harlan, Sonoma County Democratic Committee

Mr. Joseph Holder

Mr. Mark Keenberg, California Election Protection Network

Mr. Michael Keenen

Mr. Neal Kelley, Orange County

Ms. Jennifer Kidder, Elections Committee of Progressive Democrats of East Bay

Mr. Douglas Kinzle, Riverside County ROV

Mr. Dan Kysor, California Council of the Blind

Ms. Emily Levy, Brad Blog

APPEARANCES CONTINUED

ALSO PRESENT

Mr. John Longoria, Disability Rights Legal Center

Ms. Candy Lopez, Contra Costa County Elections

Mr. Dave MacDonald, Alameda County

Ms. Diana Madoshi, California Alliance for Refined Americans

Mr. Jim McCauley, Placer County

Ms. Conny McCormack, Los Angeles County Registrar, Recorder, County Clerk

Mr. Tim McNamara, Los Angeles County

Mr. Clark Moots, Placer County

Ms. Freddie Oakley, Yolo County

Ms. Gail Pellerin, Santa Cruz County Clerk

Ms. Kelsey Ramage

Mr. Preston Reese

Ms. Eve Roberson

Ms. Julie Rodewald, San Luis Obispo County

Mr. Ryan Ronco, Placer County

Ms. Bev Ross, Tehama County

Ms. Deborah Seiler, San Diego Registrar of Voters

Mr. Stuart Schy

Mr. Jim Soper, VRTF

Mr. Greg Taber

Mr. Richard Tamm

Mr. Brandon Tartaglia, Protection & Advocacy

APPEARANCES CONTINUED

ALSO PRESENT

Ms. Lisa Thomas, Placer County

Mr. Brent Turner, OVC, SFEIL, BBV

Mr. John Tuter, Napa County

Ms. Kari Vergil, San Bernardino County ROV

Mr. Steve Weir, California Association of Clerks and Elections Officials

Ms. Ann West

Ms. Gail Work, Grassroots for Bowen PAC

INDEX

INDEX CONTINUED

INDEX CONTINUED

INDEX CONTINUED

PROCEEDINGS

MODERATOR PÉREZ: Thank you for coming this morning. I'm John Pérez. I'm the Chair of the California Voting Modernization Board and I'll be moderating the proceedings today.

This is a public hearing designed to discuss the University California's red team and Accessibility reviews of 3 of California's voting systems, reviews that were conducted at the request of Secretary of State, Debra Bowen.

And I want to start off by thanking John Hancock and Jim Gualtieri and their team at the California Channel for agreeing to webcast this hearing, so that people who couldn't be here today will be able to view the proceedings on line. And if the State Senate isn't in session today or for periods of time that they're not in session, this will also be broadcast directly on the California Channel itself.

Before I get into the details of exactly how we'll be proceeding throughout the day and the guidelines for our hearing, I'd like to first introduce the Secretary of State for some introductory remarks. So please welcome California Secretary of State Debra Bowen.

(Applause.)

SECRETARY OF STATE BOWEN: Good morning. Thank you, John and thank all of you for being here today. It is quite an extraordinary day. I am moved by the number of citizens who care about democracy and the tools of democracy and who have demonstrated that concern by learning the issues, by reading reams of documents, sometimes with very short notice, and by being part of this hearing today, whether by being here in this auditorium, watching on the California Channel, watching on line, listening by conference call or by reading the reports that come from those who were here today.

Despite what are undoubtedly very divergent views on the political issues of our time, we have one thing in common. We all care deeply about our democracy and the tools that we use to ensure that our voices are heard. And our very existence as a democracy is dependent on our having voting systems that are secure, accurate, reliable, and accessible, and one more thing, they must be transparent and verifiable.

The review that I asked the University of California to conduct is intended to help us determine whether the voting systems we use meet those standards. I want to express my great gratitude to the University of California and its researchers for agreeing to conduct the top to bottom review. I also want to recognize the 3 voting system vendors who agreed, without too much cajoling, to take part in this review.

As many of you know, one vendor was so late in providing the materials we needed that it's system could not be included in the review and that is something I will be dealing with in the coming days and weeks. However, Hart, Diebold and Sequoia worked with my staff and the review team and I want to thank them for that.

My one regret about this project is time. The addition of a February Presidential Primary is a wonderful thing for California voters who want to play a role in the Presidential nomination process, but it definitely made the top to bottom review process more challenging. The testers didn't have as much time as they would have liked to review this systems. I wasn't able to give all of you nearly as much time as I would have liked between the time the reports came out and this public hearing. And I'm certainly not going to have as much time as I would like between now and Friday, which is the legal deadline for taking some major decisions.

However, extending the time line for review could have put counties in a position to have had to make changes between February and June or between June and November. Worse yet, finding out about major issues close to the February election would have left us without the ability to make certain kinds of changes and in the position of having to conduct a Presidential Primary using voting equipment known to have unresolved flaws. The implications of that for public confidence were absolutely unacceptable.

Waiting until 2010 to do a rigorous assessment of our voting systems and to make any required changes was not an option for me or for California voters. And so we have this truncated timeline.

This top to bottom review conducted by the University of California is but one piece of the puzzle. There is one thing about the review I want to point out, we did not ask the reviewers to do a forensic analysis of past elections. We did not ask them to look specifically for malicious code. Why? It's the classic needle in the hay stack problem. There are so many lines of computer code with such complex interactions that to do the review in that way would not have been a useful methodology, particularly with the time constraints we faced.

We asked the reviewers to work with a system provided by vendors and completed by the vendors as they would configure the equipment for a county about to use it in an election.

As you know, the reviewers commented often that they did not have enough time. Yet, we have learned a great deal. Instead of guessing about what the technological problems are with these systems, thanks to this review, we now know were many, though not all, of the security flaws and vulnerabilities live.

Some of the vulnerabilities that were discovered may already be protected by use procedures or mitigation measures that voting system vendors, county election officials and the Secretary of State's Office have adopted. Some of the problems discovered are new and it may be possible to mitigate those as well.

Computer programmers tell us that security is strongest when it is engineered into a computer system. And that is why the reviewers were asked to examine the voting systems without regard to use procedures or mitigation measures. That is what the University of California review teams were charged with doing, analyzing voting systems as they were certified by the private independent testing authorities and by previous Secretaries of State.

The idea of analyzing the base of the system itself to determine, first, whether it's secure and then to determine whether the system can be made secure by adding non-technological safeguards is not a new concept. It's actually a concept we use in our everyday lives. And the best analogy I can provide you with comes from something we're all familiar, the roofs over our head.

If you have a leaky roof, you can certainly mitigate the problem by putting a tarp on the roof every time it rains or by running around setting up buckets in your house to catch the water, or in certain rooms this building when it rains.

(Laughter.)

SECRETARY OF STATE BOWEN: But if you call a roofer out to take a look, the roofer is not going to look at the areas where you have not mitigated the impact nor is the roofer going to look at the tarp and the buckets. The roofer is going to look at the structural integrity of the entire roof absent buckets and tarp. Then it will be up to you to determine whether you want to pay for a whole new roof, patch the roof, move, or take whatever actions you feel are necessary, so that you wind up with a roof that does the job that you need it to do.

And that's what we've asked the UC teams to do, look at the structural and technological integrity of these systems to determine whether there are security flaws or vulnerabilities that prevent the systems from doing what we need them to do, conduct secure, accurate and reliable elections on equipment that is accessible to all voters.

The next question that we can find is whether the underlying problems can be corrected within the time and legal constraints of the certification process, whether flaws that cannot be corrected can or should be mitigated, and last where there are problems that are so significant that particular voting systems themselves simply should not be used.

I've asked a panel of 5 members of my staff to be here to formally receive the verbal report from the University of California and to receive comments from the public and the voting system vendors, because I want to bring different perspectives to the table when it is time to review and analyze all of the information that's been collected and begin making decisions.

I want to just finally remind people that this top to bottom review is not an end in and of itself. Like this hearing, it is a means to get us to a place that I know everyone in this room cares about. We want to be able to have secure, accurate, reliable and accessible elections and we want to be able to verify that. We want to be able to have confidence in the results of the electoral process.

The UC teams have gone through a thorough methodical and analytical process in conducting their examinations of these systems. And it is my intent to go through a similar, though truncated, thoughtful, methodical and analytical process in determining what to do next. And the information that is gathered from this hearing and from comments submitted through a variety of means will play an enormous role in the decision-making process. Particularly with the tight timeframe, it was very important to have many people reviewing, thinking and providing their statement. And I expect that the information that we receive today from this hearing and in writing and by Email will be critical in making decisions about what to do.

We all have a responsibility to remember that what we say and do today and this week will have a profound impact on the future of democracy and none of us should take that responsibility lightly. I would like this hearing to be as productive and informative as possible. So I hope that you will treat each presenter and public speaker with the same courtesy and respect that you have provided to me this morning.

Thank you all for coming. Thank you for caring about your democracy. I leave you in the good hands of my staff who have also worked incredible hours already and are looking at a week that's going to be a challenge.

I will be in and out as the day goes by, and look forward to hearing your comments.

John, back to you.

(Applause.)

MODERATOR PÉREZ: Thank you, Secretary Bowen.

Let me take a moment to lay out the guidelines, under which today's hearing will be operating. This is a public hearing. It's being transcribed, videotaped, carried via conference call and it's being webcast and televised by the California Channel. That means that all oral comments made here today and written comments that are provided to the panel become a matter of public record.

This is a public hearing. It is not a debate. I know that this is an issue that many people are very passionate about. However, please recognize that people have come to this hearing from all over the state of California and some from outside of the state. I would ask that you respect their opinions and public comments. Even if you disagree with them, just as you would like them to respect your opinions and public comments, when you choose to speak. Booing, hissing, applauding, shouting or other displays of support or opposition that disrupt the presenters, the speakers or the panelists are not acceptable and I will not hesitate to have folks removed from the room who can't abide by these common rules of courtesy.

If you'd like to speak during the public comment portion of hearing, you must fill out a speaker's card, which is available in front of the auditorium. And we invite everybody who's here today to make their opinions known and we invite you all to fill out a card if you'd like to speak today.

This is a public hearing where the University of California will publicly deliver a report on research it was contracted to conduct by the Secretary of State. The goal of this hearing is to have the report presented publicly, to give the voting systems vendors and the public an opportunity to publicly comment on this report, to collect information from vendors and the public that may help inform the Secretary of State in her decision of what, if any, action to take as a result of this report.

As Secretary of State Bowen noted when she was speaking a few minutes ago, even when she's not in this room, she'll be hearing the comments that are made here today and reviewing the testimony provided in the public comment by vendors, by the presenters and by the counties. And this will all serve to inform the decisions that she'll be making this week.

The panelists here today won't be voting or deciding whether to adopt the report nor will they be making any comments on the report's finding or expressing opinions on what the Secretary of State may or may not do once she finalizes her action. Rather the panel is here to formally receive the verbal report from the University of California, receive comments from the voting systems vendors and the public and bring a variety of perspectives to the issues raised in the report and by all the issues that are raised by the public when it's time to sit down with the Secretary to review and analyze all the information that's been collected.

Now, let me introduce the panel. Starting from my immediate right Lowell Finley, Deputy Secretary of State for Voting Systems Policies; Judith Carlson, Elections Division Counsel; Bruce McDannold, Interim Director of the Office of Voting System Technology Assessment; Chris Reynolds, Deputy Secretary of State for HAVA activities; and Lee Kercher, the Chief of the Information Technology Division, who will be joining us only for the report presentation and the voting systems vendor comments portion of today's hearing.

Delivering the report today from the University of California will be Matthew Bishop, Professor of Computer Science from the University of California at Davis. David Wagner, the Associate Professor of Computer Science from the University of California at Berkeley is listed on the agenda as well, because he was going to present on source code and document review reports. However, because the reports themselves have not yet been made public, Professor Wagner is not in a position to present them today.

With that, please welcome University of California at Davis Professor Matthew Bishop.

(Applause.)

MR. BISHOP: Okay. I'd like to --

MODERATOR PÉREZ: I think we have a microphone issue there.

MR. BISHOP: I'm a computer scientist, so I don't know how to work these things.

(Laughter.)

MR. BISHOP: Does this work?

Works now.

Thank you.

My name is Matt Bishop and I want to emphasize that I'm not presenting the entire report. I am presenting the results from the accessibility and red teams only.

And also, even though I'm the one up here, the work I'm presenting is the result of the an awful lot of hard work by a very large number of highly talented individuals. So what I'm going to do today or what I'm going to present right now covers only the accessibility and red team reports. The other half of the review, as was noted earlier, is the source code and document review reports, which the Secretary of State will release as soon as she ensures those reports do not inadvertently disclose security sensitive information.

I have to add that the source code and review teams did an incredibly thorough job and I want to acknowledge publicly how proud all of us on the other teams are to be associated with them.

Also, before I go into details, I'd like to acknowledge the people who actually did the work on the red team and on the accessibility teams.

The red team -- there were 2 red teams. The first one was affectionately known as Team Bob, because the leader was Robert P. Abbott. And Mark Davis, Joseph Edmonds, Luke Florer, Elliot Proebstel, Brian Porter, Sujeet Shenoi and Jacob Stauffer with the other members of the team. They were from a company called Consilium Independent Consultants and also from the University of California's Computer Security Laboratory.

The second team, which was known affectionately as Team UCSB was led by Professors Giovanni Vigna and Richard Kemmerer who co-led the team from the University of California at Santa Barbara. And the members were, and I apologize to them if I mispronounce some of these names: Davide Balzarotti, Greg Banks, Marco Cova, Viktoria Felmetsger, William Robertson and Fredrik Valeur. All of them were members of the UC Santa Barbara computer security group.

Okay. The accessibility reviewers were Noel Runyan from Personal Data Systems and Jim Tobias from Inclusive Technologies. Noel led the team.

So let me start by presenting the results of the Accessibility Study.

Basically Noel and Jim designed and ran it. UC Davis provided support. We did the Institutional Review Board review of testing procedures, because humans were involved and we also provided the videography.

Accessibility reviewers interacted directly with the Secretary of State. There were 3 types of voting systems, the Diebold AccuVote TSx, Hart eSlate and Sequoia Edges I and II that were evaluated in the accessibility review.

This review was undertaken primarily to identify whether the 3 systems were sufficiently accessible for voters with a range of different disabilities and alternative language needs. It was also tasked with identifying specific accessibility and usability concerns and reporting options both for near-team mitigations that would be appropriate for the 2008 elections, as well as longer term mitigations, including vote system design changes.

Because it's impossible to affirm overall accessibility and usability conformance, merely by examining documentation for voting systems -- or voting products and because there's never been in-depth accessibility studies performed for these voting systems, they had to do rigorous testing in order to assess the accessibility and usability of California's voting systems.

The access review test protocol used both heuristic and live user testing techniques. In the heuristic techniques or testing, experts in usability and accessibility performed many qualitative tests, including persona studies and walk-throughs and analyzing every possible aspect of the voter interface.

Live subject testing was done with 45 test voters who represented a wide variety of disabilities, attitudes, skills and preferred languages. Each of the 135 test voter sessions was recorded on DVD, both audio and video. Based on the findings of these tests, each of the voting systems was then evaluated by grading its conformance to each of the accessibility related requirements in the Federal 2005 VVSG Guidelines. The separate VVSG conformance reports for each voting system also include discussion and mitigation options for addressing the requirements that were not in conformance.

So as an example of some of the findings, one of them was although certain of the tested voting systems could be used by some voters with certain disabilities, none of the systems provided acceptable accommodations for all of the variety of disabilities voters are likely to have. Each of the tested systems had accessibility design limitations that will not allow certain voters with disabilities to vote independently.

And there were basically 3 areas of concern. The first one was physical access. Support stands for all voting systems weren't appropriate for most voters, especially limiting physical access by most voters in wheelchairs. Sip and puff and other dual switch controls for voters with severe manual dexterity impairments were lacking or not even available on some systems. In some cases, the changes made to add the VVPATs, the voter verified paper audit trails, the printers had negative impact on privacy and on the accessibility of systems for voters with disabilities. VVPAT paper trail printouts of the tested systems cannot be directly read and verified by blind voters. And they were also found to be difficult or impossible to read and verify for many other voters with disabilities.

Additionally the VVPAT printer of one of the systems was mounted, so that it blocked the approach by voters in wheelchairs and represented a severe obstruction to voters attempting to use the touch screen or reach the voter card slot.

Accessibility-related security concerns included the finding that a simple short wave receiver could be used to remotely listen to the spoken ballot of one of the systems.

Additionally, the small and ineffectual privacy panels on some of the machines were not at all adequate for preventing eavesdroppers from observing the high contrast and large print characters on the visual display screens.

The reviewers also had concerns about speech. Simultaneous output of both speech and visually displayed ballots is very important for many of the elderly and other voters with low vision, but it was not available on all of the systems -- at all on one of the systems. I'm sorry.

Speech rate control was not available on one system and that system's speech was too fast for some voters, rather like mine probably is now.

(Laughter.)

MR. BISHOP: On the other voting systems speech rate controls cause major distortion of the speech output, making the speech difficult or impossible for many elderly voters to understand. There were also concerns about the magnified text, the text that would result when you magnify the screen. One of the systems didn't offer magnified text at all. Another offered it in a way that left hidden off screen text that was easily missed by voters. Large print setup times were very long on one system, taking as long as 24 seconds to write the screen.

So the conclusions of the accessibility review folks were that because of the move up of the California Primarily election date, the scope of this accessibility testing was not as broad as desired. Further testing hopefully will be expanded to include usability and accessibility of all aspects of the voting systems, including the usability of voting systems by election officials.

As a result of the access review, it was concluded that the 3 tested voting systems are all substantially noncompliant when assessed against the requirements of the HAVA and those specified in the 2005 VVSG Guidelines. This report has documented these accessibility concerns and offered options for short-term mitigations for near-term elections and also offered system redesign options and other longer term mitigations possible for voting systems.

Hopefully vendors and local election officials may find information in this report that will improve the usability and accessibility of voting systems in both the near and the long terms.

And the accessibility review group wanted to thank Lowell Finley, Debbie O'Donoghue, Ryan Macias, Jason Heyes, Miguel Castillo, Michael Lakey, Jane Howell and Nancy Arceo from the Secretary of State's office, and I think I got those names pronounced right.

Also, the management and the staff of the grass roots organizations that helped them recruit users and the users who, in the technical sense, were subjects, but they were much more than just subjects.

Also, Stanley Chan and John Bartle of Onetake Productions were videographers who came on extremely short notice. And also Deborah Runyan Scott Luebking -- and I'm sure I mispronounced that name for which I apologize.

Okay, the second part of the study was the red team study, which, quite frankly, I was much more involved in than the accessibility study. And I wanted to first give a little bit of background, because there's a lot of misperception about what a red team study is. And then I'm going to talk a little bit about how to interpret the results. Then I'll give the results and I'll make some general comments.

One thing that I saw a lot of -- I've heard this a lot, not just this weekend but before, is that what's the purpose of a red team study? Aren't you basically just handing your keys to a car thief and saying steal my car?

And actually, it turns out that's a really bad analogy. The reason is, first of all, we're not trying to steal an election. Secondly, a better analogy is give the keys to your friend who happens to be a policewoman who specializes in the theft of cars. And you ask her, how can a thief steal my car?

Then she's going to look around the car and see if there's anything on the outside. And then she's going to ask, can I get into the car, because there may be things in the car, if the thief can get in, that will immediately allow him on her to just drive off with the card.

For example, how hard is it to hotwire a car? And that will probably, by the way, show my level of automotive expertise. And if you say well, I'm not going to give you the keys, she won't be able to do that, or she'll have to figure another way in. If she's only helping you out on her lunch hour, well, by the time the lunch is over, she can't get in.

And so it's critical when time is limited that you have access. So basically go ahead and give her the keys. She's going to tell you yeah, with these keys I can steal the car. But she's not going to stop there. She's going to say okay, let me go ahead and examine, using this protected information, what other vulnerabilities are in the car that will allow the thief to steal it if they perhaps steal the keys from you or if they're able to bypass the need for the keys and get into the car in some other way.

For example, you wouldn't expect her so smash your window. On the other hand, a dishonest thief may very well smash the window. And in that case if you can hotwire the car, you wouldn't need the keys. So that's a much better analogy.

Basically, after the policewoman, your friend, is done, you've got a list of technical ways to steal the car, use the keys, hotwire the care and so on and so forth. She's going to give you this information. Now, it's your job to figure out well, how do I prevent this? Do I, for example, get one of the alarms that goes off very loudly and annoys everyone in 500 feet? Or do I just keep the keys in my possession and make sure I don't leave them lying around where someone might take them and so forth?

And you have to make the judgment to determine what you're willing to put up with and weigh that against how the car is going to be stolen. And if you like the red team is in the role of the policewoman here. We tried to gather information that you will find useful in making your decisions.

The specific goal of the red team was to identify and document vulnerabilities, if any, to tampering or error that could cause incorrect reporting tabulation, tallying or reporting of votes or they could alter critical election data, such as election definition or system audit data.

And we basically looked at the tax that could come from everyone, from the average -- from a voter, from a poll workers, from an election official, from a vendor and so forth. We did not evaluate policies and procedures. And there were a number of specific reasons for this.

First off, we wanted to focus on the technology. We had a very limited time to perform this study. And also in California, each county -- there are 58 counties if I remember correctly, each county has its own procedures for doing things. And we couldn't examine all 58 of in the time given. And further more, we figured if we found problems, then people who know the law and know the procedures could modify the laws and procedures appropriately, if necessary, to take into account the problems that we found.

And also there's another issue as well. You can have the best policies and procedures in the world, but if they're not carried out effectively, then they're worthless. And that was another area that we did not want to evaluate at all.

We did not evaluate the likelihood of the attacks that we found what would work. And the specific reason again is we don't know what mitigations are or will be in place. We did not evaluate how serious the attacks were, same reason. We also didn't evaluate the skill level needed for each attack. And I want to spend a minute explaining why.

There are really 2 parts to each attack. The first part is devising it. The second part is carrying it out. With a couple of the attacks that I'm going to talk about, it requires some expertise to devise the attack. It requires very little to actually carry it out, once the attack has been put together.

How do you characterize that? We've decided that it would be better just to give the Secretary of State the information and let her do the characterization. We also didn't give the number of successful attacks or vulnerabilities found, because, quite frankly, that can be extremely misleading.

The numbers I'm giving, by the way, are purely hypothetical here. But let's say we had 2 voting machines, A and B. A has 10 vulnerabilities and B has 2. The immediate reaction is oh, A is much worse than B. But suppose the 10 on A could be remediated very easily by very simple policies or procedures that are carried out, and the ones on B could not be fixed?

In that case, one could argue that as part of the entire process B is worse than A. We didn't want to get into that argument, so we didn't quote numbers. The Secretary of State -- the confidential report has detailed descriptions of each attack, so they can be compared that way if you want.

And that brings me to something that's absolutely critical to understand when you evaluate these machines. The computers are part of an election process. And like any other process that uses security, you want security layered on top of layer. You want procedures. You want defensive mechanisms. You want technological mechanisms that each reinforce and support one another. This is known in the trade in different circles by different names. Defensive in-depth is probably the one most of you have heard about. It's also been called the layer Defense or in academic circles, separation of privilege.

And there's one mechanism that invariably gets cited as very effective and that's secrecy. If you keep things secret, the theory goes, you can't figure out -- the attacker can't figure out how to get in. And point of pact in our experience, that's absolutely untrue. Secrecy is acceptable as a layer. However, given the widespread dissemination of information, it's a very porous layer.

In particular, it's very hard to control information. And, as examples, I would cite 3. The first one was when the gentleman from Norway, I believe, cracked the DVD encryption mechanisms. There were lawsuits filed in the United States to block the dissemination of the code he had written. In order to do that, they had to, for whatever reason, the lawyers filed in one of their statements or pleadings, I'm not sure of the technical term, a description of exactly how the algorithm worked.

One day later, they realized that they hadn't asked for it to be sealed, so they did. In that one day, it had been posted to a large number of Internet websites and at least 121,000 downloads.

As another example, one that was much more serious, recently Fox News reported that many defense contractors had information on their websites that endangered the lives of U.S. troops. When the AP, which did the story, called the contractors, the information, of course, was immediately removed. But again, that was something that should have been suppressed and unfortunately it got out there.

The third example, identify theft. I don't think anyone would argue that Social Security numbers should be broadcast or made available to the public. Yet, we're hearing about identity theft from servers all the time.

So the bottom line is secrecy is simply a defense. It's a layer. Do not make that your key layer, because if you do, people will get through it. And the range of ingenuity that people have for getting through it is absolutely phenomenal. For example, social engineering is a good example of this. It's basically where you lie. That's probably the easiest way to do it or where you try to trick people into doing things. It's been in the news lately, except it's been called pretexting, where you illicitly get phone records.

There are a number of other wonderful stories that I tell every computer security class about this. I'll spare everyone.

So when you look at an election process, you've got to look at all aspects to it, not just one aspect of it. And in particular you've got to look at properly designed procedures and policies. If those are properly designed, those may counter many of the problems that arise in voting systems. That is again not something that the group looked at.

A word about certification. All systems used in elections in California at least have to be certified. And the standards that we were asked to look at were the 2002 Voting System Standards. And then ITAs, the independent testing authorities or agencies, I can never remember the last word. Anyway, the ITAs do the testing of the systems to be sure they conform to the standards.

Now, the quality of the 2002 Voting System Standards is inadequate. And I have not talked with any vendors about this, but I'm willing to bet they're just as confused as everyone else, that they like the standards just as much as everyone else. Again, I can point to academic papers that describe the problems.

There have also been questions raised about the effectiveness of the testing by the ITAs. And, in particular, Cyber, which was an ITA, was denied interim accreditation for testing voting systems by the Federal Election Assistance Commission, after a finding that Cyber was not following its quality control procedures and could not document that it was conducting all the required tests.

So there are issues in certification.

Now, as far as this study goes. There were 2 major constraints. The first one was the lack of time.

The entire exercise took about -- we had about 5 weeks to do the entire exercise. That is not enough to do a thorough complete -- I'm sorry. It is not enough to do a complete review. We were extremely thorough with what we did. And the exercise ended on July 20th.

The second one, quite frankly, was a lack of information and in a couple of cases vendor software. In one case some documents were delivered on July 13th. That didn't affect it too much, but we would have liked to have had the chance to get some feedback on information in those documents to see if things in there were useful. There was a lot of discussion between the red team, the document review team, the source code team and a little bit with the accessibility team. So we were sharing information as quickly as we could find it.

Some software, as of July 18th, was not delivered. And one ballot box wasn't delivered until July 18th. The software I will talk about a little bit later. I may mention what happened with the ballot box.

So what does this mean aside from the lateness? Well, what it means is the results presented in the study should be seen as, what we call, a lower bound. In other words, this is what we could find under these conditions. If those conditions were alleviated, if we had more time or the information were more complete, we may have been able to find more. And, in fact, all team members felt that they would have found more.

So we understand the constraints under which Secretary Bowen was functioning under which she commissioned a review. We just want to make it -- and we're not complaining. We just want to make it very, very clear that what we found was a lower bound.

So what kind of threats were we thinking of?

Well, there were a couple of things that are covered -- that are described in the overview that I wanted to mention. The first one is when an attacker modifies the firmware to misreport votes. The first case, you have a paper trail on all California systems. So, what you can do is inject this firmware and then when the voter votes, it deliberately misrecords one particular vote. The voter doesn't look at the paper trail -- sorry. If it prints the incorrect vote on the paper trail, there's a risk the voter might look at it. If the voter looks at it, they will discover the problem.

But here's where the fun comes in. Is it an error? Did they touch the wrong place by accident? So they go back and recast the vote. The firmware can then say oh boy, it's been recast. I've been discovered. Let me print out what they said. In this case, there will be no discrepancy, for example, between the paper trail and the non-paper trail.

On the other hand, if they don't check, if the paper trail prints out the wrong one -- sorry, if it records in memory the wrong vote and prints out the right one on the paper trail, there is a discrepancy. And this is an example of the reason why we didn't try to deal with policies and procedures. What happens in that case?

In particular, what happens if the poll books show 200 voters vote and the machine showed 400 votes on the machines? We don't know how to handle that. So in that case, we would simply report that it is possible to create this discrepancy and then it's up to the Secretary of State and others to decide how to handle that, because we don't know what the law would require.

Another example threat, and this one goes to the heart really of a lot of what we did. You have an election management system at your county seat or your elections central, depending on where you are, and it's going to run on the non-secure platform. All the vendors use Windows, for example. There the security is provided by the configuration of controls on that non-secure platform.

So this means you need to lock the system down and make it as secure as possible, so that if people attack the Windows system to get into the election management software, it will be extremely difficult for them to do so. If the attacker, for example, can gain administrative privileges on the Windows system, then they can pretty much do whatever they want. And preventing this -- and so when I say lock down, I mean turn off all unnecessary services, prevent physical access to the box, except by trusted people and so forth.

Okay, so now the moment I think everybody has been waiting for, the results. With Sequoia we were able to breach the physical security. We were able to bypass the seals and do nasty things. The firmware, the attackers were able to override the firmware. And in point of fact, this brings up a very interesting point. Windows, -- in this particular case, the vendor had their own proprietary operating system, which would make it seem more secure. But on the other hand, certain features in the proprietary operating system may be attack much easier.

The malicious firmware that the testers used was able to detect when the system was in the test -- LAT mode, when it was doing the Logic and Accuracy Tests and when it was not. So they could have -- so it could be rigged to lie to the testers.

They were able to access the election management database system directly. And from that inject malicious software onto the system. And also they could forge the update cartridges and the voter cards.

I want to emphasize read the public reports for details. The public reports go into some detail. The private reports go into a lot more detail and I would urge everyone on the Secretary of State's staff and the Secretary of State in particular to look at the private reports.

Okay. For Diebold, the election management system. The server, which was the system was delivered on, we were told was configured the way it would be configured for an accounting. It was vulnerable to well-known exploits. We were able to break -- the red team was able to compromise it using -- I don't want to say off-the-shelf, but I will say widely available software.

Furthermore, not all security related actions were logged. As far as the physical security went, the testers were able to bypass the locks. They also were able to disable the printer in such a way that the machine would continue to record votes. They would overwrite the firmware. And it turns out Diebold, to its credit, has, for a long time, a well known security key that was used. The key is the default, so if you change the system, you won't use that key. However, the default key for the

Diebold system is very widely known. Again, read the public reports.

As far as Hart goes, the election management system, this was a little bit trickier, because Hart said they would install it on whatever you wanted, which presumably meant a Windows system. So the testers did not analyze the security of the Windows system on which the electronic management software resided, because that's really some -- we felt -- the testers felt that the time could be much better spent on other things, since there was no particular configuration that counties would use.

However, they did find an undocumented account on the hard software. So in order to get access to it, you need to get onto the Windows system and then you can get to that undocumented account.

On the eScan there were able to overwrite the firmware and they were also able to issue administrative commands to the eScan. As far as the JBC goes, I need to explain something very quickly about how Hart works.

What you do is you get an access code from the JBC. It's a 4-digit access code. You then walk up and enter it on the eSlate and then you can go ahead and vote. It turns out that the access codes by using a mechanism, which is described in detail in the confidential report, we were able to get -- I keep saying we. I was around the team a lot, but I wasn't on the team. Sorry guys.

Anyway, the team was able to get the JBC to issue access codes without poll-worker intervention. If this were done in -- hang on a moment.

Okay, let me just say that in some cases it would not print out any record of -- would not print out the access codes as they were being generated.

And also, the accessibility guys clued us into this one. On the eSlate, what is known as the TEMPEST attacks succeeded. TEMPEST is a mechanism for preventing the leak of electromagnetic radiation. What we were able to do is get a small -- get an electronic listening device, stand well away from the eSlate, and since the eSlate plays audio, we were able to hear the votes as the person was casting them.

Again, I urge everyone to read the public reports, because I'm doing this orally. And the public reports give much more structure and detail to what I'm saying.

So some general comments and then a couple of lessons learned. The first one is that both teams felt that the security mechanisms on the systems were inadequate in and of themselves to ensure accuracy, integrity of the results and of the systems.

The vendors should be using, what we call, high assurance techniques. These are techniques where security is designed in from the beginning and you do a great deal of painstaking analysis and development as the system is developed. And in the overview report, there's a point or 2 if, I may say, one reasonable -- one reasonable -- a couple of reasonable chapters on it. And, of course, the fact that it's in a book that I wrote, even though I didn't write that part, has nothing to do with that particular recommendation.

The vendors, in general, should also assume that components are used in completely untrusted environments. This is not because everybody is the crooked. They aren't. This is simply another layer of defense. If you assume that these are going to be use in untrusted environments and, in fact, the people around them are trusted and no one but a trusted person uses these systems, then you've just got an extra layer in case somebody gets through that layer of trust. So I want to emphasize that. This is not an insult to anyone.

Also, policies and procedures have to be carried out and -- designed and carried out very carefully to be effective. A good example tamper proof tape.

First question, does the tamper proof tape actually cover what you're worried about?

Let's assume for the moment that you put the tamper proof tape in the right place. Do you have a procedure in place to check at the end of the day that the pamper proof tape hasn't been ripped?

The second problem, a lot of tamper proof tape can be ordered off the Internet. How do you know -- so one attack that we gamed out would be an attacker buying some tamper proof tape that looked the same as the County's. So they go ahead and tamper with the machine and then put on their own tape. How could you tell?

The proper is with serial numbers on the tape, so each strip of tape is a serial number. But then you have to have a procedure in place to check the serial numbers. So again you have to layer procedure upon procedure here.

And one thing that is rather helpful, by the way, is think like an attacker. It's very useful to say I want to try to beat the system. If I were going to beat it, how would I do it? And that starts putting you in the mindset of figuring out what to look for.

In general, and this is true, I think, pretty much everywhere, security should be part of the design and the implementation of the system. It should not be added on after the fact. The reason is when you add it on after the fact, any incompatibilities can cause extreme security problems. Or if you layer it on top of the system, if someone can get under that security layer, you're wide open.

Also, the policies and procedures should be either designed with or drive the design of the system as it's being designed and implemented. The policies and procedure should not be seen as separate from the system. They should be seen as an integral part of the use of these systems. Again, election is a process.

And although it may be a little bit -- also the testers -- the red teams did have a recommendation to the Secretary of State. If you plan to do this again, we would strongly urge you to adopt regulations to require the delivery of everything needed to conduct the tests like this before certification or before you do the testing, that way the testers can drive right in and won't have to wait if there are miscommunications or issues?

And that pretty much summarizes the red team review. I do want, however, to express thanks -- the red team, me personally, do want to express thanks to Jason Heyes, Ryan Macias, Miguel Castillo and Chris Maio for taking care of the systems and us. These red teams typically do not work 8 to 5. It's usually more like 8 p.m. to 5 a.m. And they were absolutely troopers in making systems available to us.

Debbie O'Donoghue and Lowell Finley were wonderful with administrative support in helping us communicate with the vendors. Again, the red teams all want to express their extreme gratitude to the source code review team members, the document review team members and the accessibility review team members, in particular all the members spent -- the source code and document review teams spent time with the red teams, and in some cases helped the red teams develop and carry out the attacks.

And I would be remiss if -- I also would like to thank Professor David Wagner of Berkeley. David's been one of the strongest points of this project. It's been a delight to work with him. He did an absolutely amazing job as did all of his team members.

And I think that's the -- for the rest of it, it's on the web. I guess it's still on the web, isn't it?

You can read the overviews and the public reports of the 3 machines.

Thank you very much.

MODERATOR PÉREZ: Thank, Professor Bishop.

(Applause.)

MODERATOR PÉREZ: Here's what I'm going to do.

MR. BISHOP: I'm sorry, I should ask if the panel has any questions.

MODERATOR PÉREZ: Yeah, I'm going to walk us through that. We're going to take a little bit of time now to have each of the panelists be able to ask any clarifying questions they have that they think will either help them clarify their own understand of the information or that they think will bring greater clarity to the audience both here in person and listening in.

So what I'm going to do is just moderate and allow everybody to just raise their hand and be recognized to ask questions of Professor Bishop. This is not going to be a debate format. Again, this is just clarifying questions. And it will start us in getting the clarification we think will be necessary to move forward.

If the panelists haven't already done so, if you'd just turn on your microphones. By holding down the mute key for a few seconds, your microphone will come on.

MR. BISHOP: They're not computer scientists so they'll probably do it right.

MODERATOR PÉREZ: So, Lowell, would you like to start us off?

PANEL MEMBER FINLEY: Sure. Thank you.

Is it on?

MR. BISHOP: It's not just computer scientists.

(Laughter.)

PANEL MEMBER FINLEY: How is that?

MODERATOR PÉREZ: Take mine?

PANEL MEMBER FINLEY: First, I want to thank you for an excellent presentation and for your overview report on the 3 red team reports, which I think helps everyone to understand them better.

The way we can tell you're an expert is that you use undefined terms because you assume everybody knows what they mean.

(Laughter.)

MR. BISHOP: My apologies to all for that one.

PANEL MEMBER FINLEY: So I just wanted to ask you to explain a couple of things. You referred several times in your presentation to firmware. And perhaps you could explain what firmware is as opposed to all the other kinds of ware kinds that we take about with computers.

MR. BISHOP: Hardware are the chips and the silicon and the physical box. Firmware is a type of software that runs on these particular machines and software is like the election management systems and so forth.

PANEL MEMBER FINLEY: So when you say firmware runs on these particular means, are you talking about the voting units?

MR. BISHOP: I'm sorry, yes the voting units and the eScan and the AccuVote-OS. And I believe it's the Insight OS. And also the touch screens and the eSlate, which -- and the JBC which are not quite touch screens.

PANEL MEMBER FINLEY: Which leads me to my next questions. You mentioned the eScan and the OSs for the other 2 vendors systems. Can you explain what those are?

MR. BISHOP: I'm sorry. eScan and the other systems that I named in conjunction with them are optical scan systems. You basically have a scanner and you feed your ballot in and the machine scans the ballot, records your votes and then dumps the ballot into a ballot box underneath.

PANEL MEMBER FINLEY: Okay. And then you also referred during your talk to the JBC in the Hart system. Can you tell us what that is?

MR. BISHOP: Yes. The way the Hart system works is at the polling station you have a machine called the JBC, Judge's Booth Control, and that's connected to another machine called the eSlate. There may be several eSlates daisy-chained in a row talking to one JBC. And when you go to vote, the poll worker will walk up to the JBC and ask for an access code. And it will, at least on election day, it will print out a little piece of paper with the access code. You, hand it to the voter. The voter walks over to one of the eSlates connected to that JBC, and then using a dial, dials in -- a dial-in push button selects -- enters the access code.

At that point, the eSlate will communicate with the JBC and basically say is this one active? And if the answer is yes, it will go ahead and let the voter vote.

PANEL MEMBER FINLEY: And when you were describing the JBC and the attack in which it was possible to get the JBC to issue multiple voter access codes, what was the ultimate effect of that in terms of what it enabled the attacker to do? I'm not sure that I heard that.

MR. BISHOP: If you didn't hear it, it's probably because I didn't say it. The attacker would have multiple access codes, so they could vote multiple times.

PANEL MEMBER FINLEY: Thank you.

MODERATOR PÉREZ: Thank you. Next Judith, did you have any questions for clarification?

PANEL MEMBER CARLSON: I don't, but I'd just like to thank you for your report.

MODERATOR PÉREZ: Very good.

Bruce.

PANEL MEMBER McDANNOLD: Thank you, also, Matt, for the hard work you and your team did -- two of your teams did on this.

Can you elaborate a little more on -- you've talked about very briefly mentioning a couple times in passing that you were able to overwrite the firmware.

MR. BISHOP: Yes.

PANEL MEMBER McDANNOLD: Can you elaborate on the potential consequences of doing such an act, not just particularly for the current election, but for perhaps the future?

MR. BISHOP: To be honest, I can't really relate it -- I wasn't really relating to any particular election. Altering the firmware allows the malicious -- allows the program that is added to control the system completely. For example, when a vendor goes to do an update, they alter the firmware. The attacks that we were talking about, in fact one that I mentioned, allows a nasty person to alter the firmware in such a way that the wrong vote will be recorded. And then if the user spots that the wrong vote has been recorded, in other words, they don't cast the ballot, what they can do is -- what the software can then do is say, "Oh, gee. I may be detected. Let me be honest this time." And you can play those -- form those sorts of tasks.

On other systems what you might be able to do is, for example, change how things are counted. So in other words, you could alter how the systems function. Does that make -- so in other words, if there were 3,000 votes for John Doe and 2,000 votes for Jane Roe and you wanted to switch them, you could do so. Depending on how the software worked, that might or might not be apparent from the paper trail.

Actually, let me rephrase that. I don't think any single electronic voting machine has a history of the 3,000 or 2,000 votes, but I think you have the idea. It would be like maybe 100 or 200 or however many, but you could switch things.

PANEL MEMBER McDANNOLD: And, again, were there any -- having access to alter the firmware, does it have implications for future elections that are run on that system?

MR. BISHOP: If the firmware is not reflashed or not fixed, then the corrupted firmware will continue to run on that machine, so it depends on your policies and procedures. And this is one of the reasons why the report is so careful not to draw conclusions as to the effects of specific things we find. We simply considered them from the point of view of technology. And we make statements about what the technological implications are, but not what the implications are for elections, because it depends on the compensating controls.

PANEL MEMBER McDANNOLD: Okay.

MODERATOR PÉREZ: Any other questions, Bruce?

PANEL MEMBER McDANNOLD: Not for now.

MODERATOR PÉREZ: We'll come back to everybody if other questions come up.

Next, we have Chris Reynolds.

PANEL MEMBER REYNOLDS: Hi. I just want to thank you again, as everyone has. It was a very thorough presentation.

I wanted, I guess, to try to get some clarification too on those things that you mentioned were not addressed in the review. In other words, you mentioned several times that you did not review the policies and procedures.

MR. BISHOP: Correct.

PANEL MEMBER REYNOLDS: And those might be policies or procedures that would mitigate against something occurring.

MR. BISHOP: It's entirely possible. We don't know.

PANEL MEMBER REYNOLDS: And then you also mentioned, in less detail or fewer times, I guess I'd say, you didn't assess the degree of difficulty for the attacks, but you did elaborate on that by saying it might be very difficult to design an attack, but easy to implement one. Is there any way you can elaborate on in helping us understand that?

MR. BISHOP: I can give you a very good one. If you remember the firmware attack that I just described for Bruce -- or sorry, Mr. McDannold. The creation of that requires some knowledge of how the systems work. It's not something your average voter will be able to do. However, actually carrying it out would simply require access to one point at the election process. And anyone who had access to that point or who was able to get access to that point would be able to carry out the attack.

On a much more mundane level, one of the locks that was opened or that was bypassed, the first time the red team tester tried it, we'd not seen this particular type of -- we'd not seen this particular situation. The tester was able to bypass the locks, I believe, in about 5 seconds. At that point, something which we christened the observer effect, came into play. He called a bunch of people over and tried to do it again. It took him 2 and a half minutes.

So, again, the policies and procedures, if there were a procedure whereby someone were watching and they noticed someone fiddling around with the lock for 2 and a half minutes, one I would hope the poll worker would come over and say, "Excuse me, what are you doing?"

Okay. So that's an example of the types of procedures we didn't evaluate. And that's also an example of why we didn't evaluate the difficulty, because the first time the person did it very quick. The second time the person did it, very hard. How do you evaluate that?

PANEL MEMBER REYNOLDS: And could you -- again, this is for clarification purposes for my own. Is what you just described, though, an illustration of layering. You described that you might need to have knowledge of the system to be able to design, and then in order to carry it out, you'd have to be able to get -- it would be relatively easy, but it might be observed or -- and in each one of those cases I'm imagining it would be things like limiting knowledge of the system, limiting access to the system, and then doing some kind of observation of what's going on in the polling -- I mean --

MR. BISHOP: Well, let me give you an answer, but like any true professor, I'm going to weasel a little bit.

First of all, the short answer is, yes, what there -- that describes layers. The first layer would be trying to keep information about the system relatively hidden. The second one would be trying to limit access to that point in the process where you could do the injection. The third one would be having a condition -- having people check for that sort of thing. The 4th one would be within the system itself, building it so that if malicious software were injected into the system -- or unauthorized software were injected or unauthorized firmware were injected, the system would say hey wait a minute. This is wrong. Stop. So that's the example of layering.

Now, I want to emphasize again, the first layer was strictly knowledge of the machine. Personally, I think that is a very, very difficult thing to do and it should absolutely not be seen as a key layer, okay. It's a barrier. But on the other hand, it's a barrier that, in this day in age, is typically very, very easy to overcome. So I very strongly want to reemphasize that that's probably -- if you think of a brick surrounded by paper, that's the paper. The other layers should be the brick.

PANEL MEMBER REYNOLDS: Add one last question. Is auditing in any way a part of the layering or is that more --

MR. BISHOP: Yes. Auditing is a very important part of the layering. And, in fact, it's an important part of the security, because systems, in general, need to be designed. With security you always prevent. However, prevention fails. I've never seen a system yet that someone has not been able to get through, so you build auditing mechanisms in to detect when that happens. And if you can't react fast enough, hopefully the audit records will show you exactly what happened and how to fix it. How to fix it or prevent it.

So this should be designed in with the system from the beginning. It's just another security mechanism. And the auditing itself is simply another layer.

PANEL MEMBER REYNOLDS: Thank you.

MR. BISHOP: Layers upon layers.

MODERATOR PÉREZ: Thank you. Lee.

PANEL MEMBER KERCHER: I have no questions.

MODERATOR PÉREZ: Please, Mr. McDannold.

PANEL MEMBER McDANNOLD: In a lot of these security analyses, people will often make a distinction between attacks that can affect one machine perhaps in the vote results on one machine versus attacks that have the potential of systemic consequences and affecting the whole system. Can you, in any way, kind of just briefly touch back on your findings and your team's findings in terms of which attacks and differentiating between them?

MR. BISHOP: I'm not really comfortable doing that without going into the private reports.

PANEL MEMBER McDANNOLD: Okay. Fair game.

Thank you.

MODERATOR PÉREZ: Thank you.

If you want to take a minute or 2 to add anything that maybe has come to your mind that isn't necessarily a direct response to any of the questions, but you think is important for everybody to hear, this is your opportunity to do that as well.

MR. BISHOP: I'd just like to thank everyone for the opportunity to participate in this. And that also again I'd like to thank every one member of all of the teams, and particularly David Wagner for an absolutely fantastic job. If I could work -- if I ever get to work with him again, and I dearly hope I will, it would be an honor and a privilege.

MODERATOR PÉREZ: Thank you very much, Professor Bishop.

(Applause.)

MODERATOR PÉREZ: We've now come to the portion of our hearing that we've set aside for the vendors to respond to issues raised by the report. We've allocated 30 minutes for each of the voting system vendors to provide any comments they'd like to make on this report.

The agenda lists Diebold as the first presenter, followed by Hart and Sequoia. However, if the companies would like to rearrange the order of their presentations, I don't have any objection to doing so.

When they're done making their presentations, again the panelists will have an opportunity to ask clarifying questions. And then later in the program, we'll open it up for public comment for everybody who's here this morning.

So with that, if I could have, first, the representative from Diebold, unless the vendors have made other arrangements. I believe it's Mr. Norcross, is that correct?

MR. NORCROSS: Yes.

MODERATOR PÉREZ: And if you'd take just a moment to introduce yourself to everybody with us this morning and then get into your comments.

MR. NORCROSS: I will.

Mr. Pérez and panelists, thank you for the opportunity today to present Kathy Rogers' statement. My name is Rob Norcross. My firm represents Diebold Election Systems. Kathy Rogers is the Director of Government Relations for Diebold Election Systems. Unfortunately, storms in the south eastern part of the country yesterday forced several airports to close and resulted in the cancellation of hundreds of flights.

Because I happened to fly out to California yesterday morning on other business, I'm able to be here today to read Kathy's statement.

> "Thank you, Secretary Bowen, for the opportunity to be here today to provide comments on the review of Diebold Election Systems Solutions commissioned by your office and undertaken by the auspices of the University of California and others.
>
> "Many jurisdictions in the State of

California use our optical scan and touch screen election systems. We are proud of our customers' records of successful elections and also very mindful of the challenges that we have faced in California in the past. We believe that we have an obligation to our customers and to the voters of California to continually review and enhance our voting systems.

"Furthermore, we believe that when used in conjunction with proper security procedures and protocols, our voting solutions encourage voter participation, help reduce voter errors and ensure good elections.

"Election day parallel monitoring testing, performed on DESI voting solutions in California, as well as in other states, have shown them to be 100 percent accurate during those elections.

"Diebold received a copy of the public reports portion of the review Friday afternoon. Our engineers and technicians are thoroughly reviewing the report and plan on providing detailed comments with your staff when they sit down to review the private portion of the report later this week. While we believe there was merit in participating in the review, we shared with your office in a letter dated June 6, 2007 steps that could have been incorporated in your test that we feel would have enhanced the value of the end result.

"We believe the process would have been enhanced if the testing team included an experienced election official. We were disappointed the California laws and regulations regarding the use of voting systems were not applied to the tests. As was stated here today, all voting systems in a laboratory environment are vulnerable, including touch screen systems, paper-based optical scan systems and the older lever and punch card technology that they replaced.

"Unfortunately, under the rules and guidelines established for the review, Diebold was not allowed to submit the testing, the most recent version of its software and firmware. In February 2006, the University of California at Berkeley and others performed a review of the DESI voting system software and found risk issues. Diebold upgraded the software by adding several new features. The software has been federally certified, but has not yet been certified in California.

"As a result, the risk issues reported by the UC Berkeley and others team and corrected by Diebold will be reported yet again in the top to bottom review.

"Notwithstanding these observations, we are pleased to participate in the review. We enjoy a cordial and professional relationship with your staff and members of the top to bottom review team. We look forward to our ongoing discussions and to working with you to further enhance the security of Diebold's election solutions for our customers and the voters of California."

MODERATOR PÉREZ: Very good. And actually, I'll turn to the panelists now and ask if your preference is to ask clarifying questions individually or whether you'd like to wait until we've heard presentations from all 3 of the companies?

PANEL MEMBER KERCHER: Now.

MODERATOR PÉREZ: I'm sorry?

PANEL MEMBER KERCHER: Now.

MODERATOR PÉREZ: Very good. So we'll do them one by one.

Mr. Kercher.

PANEL MEMBER KERCHER: Not a chance.

(Laughter.)

MODERATOR PÉREZ: Pass it down. I'll turn it on for you.

PANEL MEMBER KERCHER: Your comment that -- and this may put you in a bit of a difficult position, because I know you're not reading your own material. But you commented that the testing was not done on the most current version of firmware and software for the product. Do you have a -- can you give us a sense of how much different the results might have been if it had been done on current software and firmware

MR. NORCROSS: Personally, I'm not sure. What I can tell you, and in the brief conversations that I've had with the Diebold people when they asked yesterday if I'd be willing to come read this statement, is that many of the -- and Ms. Rogers really intended to be here and is actually on an airplane right now. She's spent over 12 hours in the Atlanta airport yesterday trying to get here.

Many of the comments that were in the UC Berkeley report from February 2006 are similar to the comments in the public section of the top to bottom review. And the Diebold folks have spent a year and a half attempting to mitigate those, so I would believe that many of them would have been addressed.

PANEL MEMBER KERCHER: Okay.

MODERATOR PÉREZ: I'm used to being Chair and not moderator, so I'm going to step out of my role a little bit and take a moment of privilege, because I have a follow-up along those lines. And the question is this, the new firmware and software that you're referring to is not in use anywhere in California though, correct?

MR. NORCROSS: That's correct. It has not been certified.

MODERATOR PÉREZ: Thank you.

Anybody else have any questions for Mr. Norcross?

Okay, thank you very much.

MR. NORCROSS: Thank you.

MODERATOR PÉREZ: The next presenter we have is from Hart Intercivic. And if the Hart folks would like to come forward and introduce themselves.

MR. McCLURE: Good morning my name is Neil. I'm with Hart Intercivic. I want to thank you for the opportunity to speak today.

The eSlate system, our electronic voting system, was introduced in the summer of 2000 following a 3-year development effort. The system was first used in the 2000 election. Since November of 2000, the system is now installed in over 300 jurisdictions and 11 different states, and a couple of the largest counties in the country that have implemented electronic systems.

Since the initial introduction of the eSlate system, we have released new system applications to support storage and warehouse management, distributed collection of cast vote records, candidate rotation and multiple language support. These features along with other upgrades to our applications represent the focus of our development resources over the first 3 years of the system's life.

In 2003 it became clear to Hart that the public demanded higher security for electronic voting systems. Since no standards were in place and some key policy decisions had not been acknowledged or addressed, Hart nonetheless set out on an accelerated development program in an effort to implement additional enhanced security features, many of which were part of our original architecture.

Despite the lack of guidance from the election industry, Hart made a substantial investment in 2003 and embarked on a focused development effort to incorporate current information technology techniques using industry best practices to implement a high security architecture for the Hart voting system.

To assist us in the achievement of this goal, we retained the services of a respected company in the applications security industry whose name is @Stake who have subsequently been acquired by Symantec and is part of their professional services group. Security is not a one-off effort but an ongoing commitment that is integrated into the business process of a company.

Hart Intercivic structured development environment and our ISO certified quality of facility securities systems were an ideal foundation to integrate security practices within our organization. The @Stake representatives spent 1 month on site in our facility conducting interviews and engineering staff, reviewing code, revising business processes while assisting us in integrating the security culture to the Hart voting system.

The first effort completed by the Hart/@Stake team was to define a framework for a threat model for electronic voting systems.

A threat model attempts to encompass as many factors as possible surrounding the operation of a system. A threat model is not just about technology, but includes other system-relevant elements, such as operating environments, characteristics of typical users, functional requirements and the motivation of hackers or attackers to name a few.

The intent of threat model is to define the environment so the system can be applied for evaluation of potential vulnerabilities, mitigation, procedural requirements and other elements that collectively make up the security architecture.

System security is not a yes or no question, but it must be evaluated in terms of probabilities and likelihoods. So without some form of threat model, there's no reference frame to perform a security assessment. Furthermore, implementation of security features can have significant impacts on system cost and usability. Higher security typically results in increased system costs, increased operating costs, increased complexity, yielding reduced usability.

The threat model helps to evaluate these trade-offs as system designers attempt to find acceptable and reasonable balances between these important aspects.

The red team explicitly states that no threat model was used in their testing. Without quote making assumptions about compensating controls or procedural mitigation measures that the vendors and the Secretary of State or individual counties may have adopted, the findings of the red team are not surprising.

The outcome is made further obvious by the fact that the red team was provided all technical information including source code of the system. But by ignoring the operational environment, the red team tested the system out of context so as to take actions based solely on their findings would produce unrealistic results, generating unintended consequences and potentially reducing the overall security of the system.

The red teams also highlight where trade-offs were made in the face of system costs and usability. Several suggestions were made in the report that can raise the level of security, but the real question is whether it's necessary. Is the cost benefit ratio acceptable when applied to the probability of a successful attack? Cost to define both a system cost and increase in complexity in the system operation.

This really points for the knead to develop and adopt a threat model so that vendors, election officials and the public have common reference points for voting systems security. Until a threat model or at least key aspects of operational environment can be agreed to by the industry, there will be no agreement on what is reasonable or acceptable security. These key aspects of the operational environment also need to be applied equally to all types of voting methods as well, including electronic, optical scan and paper ballots.

The electronic systems have typically been held to an absolute standard, which is unreasonable while the a vulnerabilities of other voting methods have been ignored.

Without some agreed to parameters surrounding security, the security debate will continue without resolution, and all parties will suffer, including the public through their lack of confidence in the U.S. election process.

This is exemplified by an illustration from our security development effort. Since their is no standards or guidance provided by the election community, Hart needed today define an operating environment to establish some binding parameters for our security protection. In order to make these decisions and have some form of reference, we analyzed what had been practiced and accepted for many years for paper ballot voting methods.

Some fundamental results from that analysis were that the polling places were supervised and trusted. The elections central office is supervised and trusted. And information, while in transit, is at risk.

These are the same conditions that are and have been used for paper ballots for many years and are reasonable assumptions that can be stated for electronic systems.

Naturally, when the red team testing was not subject to these conditions, perceived vulnerabilities will be discovered. A case in point is Attack Scenario 1 in the public report where additional access codes were allegedly gained by a malicious voter using a surreptitious device. This attack requires a distracting of a poll worker for a significant amount of time to physically plug in a device to the back of a piece of election equipment that sits in full view of the entire polling site and to do so undetected. After being connected for 30 seconds, the malicious voter removes the device, again undetected.

In the Hart voting system, an access code simply allows access to a particular ballot style that can be voted at an eSlate device. Having the access code is identical to having a blank ballot, so that the same vulnerability exists for paper systems, but the attack on a paper system requires a malicious voter to only distract the poll worker for a few seconds, enough time to steal additional ballots.

There are some inconsistencies in the red team report surrounding this attack, and we need to investigate them further with the red team. The JBC prints access codes for early and election voting modes. And the access codes are not active until they are printed.

From the description of the report, we aren't clear how the attack is successfully carried out once the access codes are surreptitiously collected as the access codes are not active themselves.

The threat model also takes into account technology, operating environment and human factors. To address the premise that information is at risk in transit, we need to use some form of cryptographic keys. When faced with the use of cryptographic keys, we are challenged by our customers experience with the use of such technology or anything similar.

Enough challenges exist with poll workers and we determined it would be an unacceptable situation to require poll workers to be responsible for private encryption keys.

The risk to a system when introducing a

cryptographic key in infrastructure is that the system can be rendered inoperable if the keys are not managed properly. This is why we chose a symmetric key pair to authenticate information at the termination of transit. Symmetric keys are easier to manage and provide a reasonable level of security when evaluated within a threat model. Yes, our system can support public/private key pairs.

Yes, it is a stronger security. But is it a requirement? Is the increased complexity a trade-off that will be understood by the public, understood by the customer when they get out of synchronization and renders the system inoperable in the name of stronger security?

We don't have the answers to these questions and that's why we need to work together to resolve these issues.

This also raises an interesting issue worth consideration. The vendor community has been asked to develop increased security for electronic voting systems ahead of the establishment of standards or determination of other public policy issues. The issue of authentication versus encryption is an excellent example of a public policy that vendors have been forced to answer without guidance from the election community.

Is ballot data public information?

If so, can it be obscured from public view?

We've been asking these questions for several years and have received no definitive answer from the election community. We generally believe it will only get answered in a court some day.

In the absence of guidance from the election industry and not wanting to be part of the judicial test, we took a conservative position on ballot data that is public and cannot be obscured from view. Hence, our system security is built on the premise that information can only be digitally signed and authenticated, visible, and not encrypted, obscured, for transfer between locations.

Is this the right decision? We've been asking these questions and trying to find a venue to have these discussions. And hopefully these are avenues that we can move forward with the red team and with the Secretary.

We understand also that the red team was given a limited amount of time to which to test our system. Our preference would have been to provide some level of training on the use of the Hart voting system as we believe it would have saved time on the learning curve and made them aware of other features of the system.

An example of this is in regards to our application called SERVO, a system application that provides equipment management warehouse functions, data backup for voting devices and system verification. This latter function of system verification was not apparently understood by the red team. One of the fundamental security elements of the Hart voting system is the distributive storage of the cast vote records in physically separate memory devices. The Hart voting system was designed such that there are 3 independent storage locations creating triplicate originals. For the DRE this includes our memory device that's removable, the JBC and the eSlate. And for our digital scanner, it includes the memory removable device, the eScan unit itself and the paper ballot.

It can be practically guaranteed in the context of an election that at least 2 of these storage mediums will be under separate custodial care and travel different pathways back to election headquarters. As mentioned above, SERVO will back up the data stored in the hardware devices, other than the MBB and that contain original cast vote records. SERVO also reconstructs MBBs with data contained on JBC, eSlate and eScan to create duplicate MBBs.

These duplicate MBBs can then be read by tally, the tabulation application, to produce a second set of original results that are compared to those that were produced from the MBB that traveled a different pathway. This is not a lengthy audit process and can be provided on election night or when the equipment is backed up. The dysfunctional capability nullifies the Attack Scenario 2 contained in the report, where the malicious voter or individual removes the MBB from the JBC, breaking seals and violating other procedural issues, modifies the information and puts it back in. There's 2 other storage locations that exist that would dispute the results on there. And in order to successfully manage this attack, all of those memory locations not only need to be altered but altered identically.

It's been a difficult couple of years for the vote system vendors. Federal attention, new standards, requirements for additional voting methods, accelerated time frames, media focus and the whole community of election experts presented new challenges as it would for any company in any industry. Federal officials, State officials, public outcry, academic community and a thirsty media all with different perspectives, objectives and agendas all pointing at the vendors to solve individual problems.

County officials understand the importance of working with vendors to solve our election issues and there are some lessons to be learned from this working model.

But being forced to work in a vacuum will never solve these issues faced with the election community, so we need to come together and solve them as one.

We congratulate the Secretary and the red team for their effort. However, we may have handled it in a little different manner if we had input into the process. Hart had spent a large sum of money on the development of the security infrastructure who had nobody to review it that would yield a credible outcome in the view of the public. If Hart paid for the review, it would have tainted the result in the eyes of the vocal critic's electronic voting. Voting system standards are behind and haven't kept pace with the new security requirements demanded by the public.

We'd also like to point out that the attacks are defined as single point attacks and do not account for the interlink nature of parameters within our system. For example, over-written firmware is the something that would be detected if run in a normal election cycle.

We'd like to suggest some possible approach for the future of such reviews and would be interested in helping you establish a national program that would be satisfactory to all interested parties.

The biggest issue surrounding open inspection and review of our system by third parties is disclosure. We have a duty to our customers and the public to protect the integrity of the system. This includes being mindful of the possibility of malicious claims being made that are not factual, defamatory or other wise intended to promote an alternate agenda.

We are interested in continually improving our system. And an excellent source of input is from third-party independent reviewers. However, it's very difficult for us to agree to open inspection if we're not allowed time to address any findings resulting from the inspection before being made public. This is not in the best interests of our customers or the public. We'd like to suggest that we open -- that we establish an open inspection protocol that be based on a model developed by the Organization for Internet Safety and detailed in their guidelines for security vulnerability and reporting and response document.

The process developed by those member organizations is a multi-step process, where a vulnerability is identified confirmed and then the clock starts ticking down toward a disclosure date. Our biggest concern with an independent review is being provided an appropriate amount of time to address any issues discovered prior to public disclosure and agreeing to such a review without the opportunity to address issues Jeopardizing the integrity of our product and is a disservice to our customers and threatens public confidence.

We understand public disclosure is a leverage historically used to motivate a manufacturer to correct the problem, but it must be used responsibly to conduct an open inspection in a cooperative manner.

There is also an issue of funding ongoing conduct of open inspections. The vendors can't pay for the reviews as it will taint the outcome. States and counties don't have the budget for ongoing financial support. Short of a federal appropriation, there's another possible source of funds.

If we, the election community, develop a clear, concise, documented process for the ongoing effort of independent third-party open inspection of voting systems, we believe there are a number of philanthropic organizations whose charter is to fund efforts for the public good and this program may well fit within their guidelines.

This solution is worth pursuing, but it requires cooperation of all parties to work towards an acceptable process.

The current red team report of their findings and related observations, require additional review and discussion between the team and our company. We have found several inconsistencies, alternate conclusions, omissions and a few errors in the report. It is critical that these be addressed before any action be taken on the report.

It was also disappointing that some of the well-designed security aspects of system were not acknowledged.

We look forward to continuing to work with the red team to address unresolved open issues in the report. We agree with the Secretary that this process is not complete and that with the red team and the Secretary applying an operating environment to the system, so that responsible actions, if any, can be identified or result of this review.

This report is an important tool, but must be used responsibly.

Thank you for time.

MODERATOR PÉREZ: Thank you, Mr. McClure.

(Applause.)

MODERATOR PÉREZ: Any questions from the panel?

Okay. Seeing no questions from the panel, thank you very much, Mr. McClure.

We're going to have a final presentation from the representative from Sequoia. We'll engage in questions from the panel for the representative from Sequoia. I'm then going to layout some of the rules for the public hearing for everybody else's participation. We will take a break after I've laid out those rules to allow people to have lunch. I'll establish a time for us to reconvene and then we'll take as much of the afternoon, and if need be, into the evening to make sure that everybody is here today that wants to be heard is able to speak on the issue.

So next we have a representative from Sequoia. And I believe it's Steve Bennett?

MR. BENNETT: Correct. Madam Secretary, members of the panel, members of the public and also members Of the California county clerks, recorders and registrar of voters that are in attendance today.

My name is Steven Bennett. I represent Sequoia Voting Systems. I'm going to read a response -- or our initial response to the red team penetration testing and accessibility portions of the Secretary's top to bottom review of Sequoia's voting equipment currently used in 21 of California's 58 counties.

Nothing in life happens in isolation. As we have stated many times, as have our nation's election officials, elections are complex systems made up of not only election equipment, but the people and the process surrounding the equipment. California's top to bottom review was conducted in a true -- was not conducted in a true election environment in accordance with ISO 15804, Common Criteria for Information Technology Security Evaluation and/or ISO/IEC 17799-2005.

This was not a security risk evaluation, but an unrealistic worst-case scenario evaluation limited to malicious tests, studies and analysis performed in a laboratory environment with computer security experts with unfettered access to machines and the software over several weeks. This was not a real-world scenario. It does not reflect the diligence, hard work and dedication to the stewardship of our nation's democracy that our customers and all election officials carry out every day in their very important jobs of conducting elections in California and throughout the United States.

As stated by our company many times in the past with a verifiable voter paper audit trail, that was pioneered by Sequoia in actual elections in 2004 in post-election checks, that are already established by law and regulation, none of these attacks described in the red team report are capable of success. All would be prevented or detected through the use of VVPAT and legal sufficient audits. Red team penetration testing is a well-known technique in the security industry. It is normally performed in a manner by which the system, in its native operation mode, is subjected to attacks from the red team, which is given various levels of knowledge regarding the system based on what the team is expected to emulate, inside threats, outsider threats or ad hoc.

In this case, the stated objective was to emulate both the insider and outsider threats. However, the test plan actually employed suffers from the misapplication of this methodology. The red team has no corresponding blue team, a friendly study, a system under study, to emulate traditional and current election security practices. In short, the red team was able to, using a financial institution for an example, to take a lock off the front door of the bank, remove the security guard, remove the bank tellers, remove the panic alarm that notifies law enforcement and to have slightly limited resources to pick the lock of the bank vault. Such a scenario is implausible.

Furthermore, the equipment tested was not taken through the prescribed pre-election logic and accuracy testing and preparation, which would have included the addition of tamper evident sales. These seals, for example, would have precluded many of the attacks on the system.

The methodology used implies that election authority insiders have unlimited access to the equipment with no surveillance of their activities through automated methods. This is untrue. The election jurisdictions have several methods of insider deterrence and apprehensions. These include cameras in the election warehouse and computer rooms, audit logging on election database servers and workshop -- and work stations, and laws that make tampering with election equipment a felony in both state and national level.

In summary, a more effective test would have been for the red team to have attacked simulated target jurisdictions. Said jurisdictions would have prepared the equipment for keeping with traditional current and legal mandated equipment and procedure safeguards. The results of this test would have pointed out the true weaknesses in election process security and provided real data from which the Government could have improved the security profile. As it stands today, all that we have proven is that computerized systems removed from the environment and place, in this case almost literally, out into the street into a laboratory for anyone to tamper with, can be successfully attacked. The data is thus unfortunately muddled by the appropriate test methods forcing governments to separate the wheat from the chaff of the ramifications for secure elections.

Sequoia will address each and every attack scenario in the red team report, its implications, mitigations, as well as the points in the accessibility report.

In this presentation today, I will go through many of these points with you at a high level summary to give you examples of the interest of our allotted time to present here today.

We will share more information this week in response to both of these reports. As for the Accessibility Report, Sequoia's equipment complies with the requirements of the current 2002 Voting Systems Standard, as well as California's State requirements. Sequoia's worked with both the national and local accessibility groups to design our voting system and we continue to do so in an effort to make our voting equipment as accessible as possible and continually improve our products to advance our main -- and to improve our products as advances are made in technology to better assist persons with disabilities.

We appreciate some of the information and feedback contained in the accessibility report. However, many issues raised are not deficiencies in the system design, but rather a function of the feedback that we had received throughout the national and local groups.

Going back to the red team's report, these describe mitigations directly address each listed issue that the red team took with the Sequoia system. The mitigations fall within categories defined in ISO 27001, Information Security Management System, ISO 27001, as an international standard, valid in over 150 countries for the protection of information and information systems.

The ISO standard includes security practices around risk management, personal screening, computer network security and business continuity disaster recovery. Sequoia recommends that all government involved in elections consider ISO standard and its companion guidance document ISO 17799-2005, when enhancing the security of their elections.

As an example of the issue, we take with the red team report in the introduction portions of the report, the investigations defined the insider and an outsider and note that where system security relies upon proper application of procedures, it may be appropriate to examine the consequences of any failure to follow procedures. There are underlying automated systems, security cameras, server and client audit logging, that are present. The report takes none of these security systems into account in providing its results. Sequoia does concur that red team attackers should have knowledge of the system in order to simulate the patient or a well-resourced attacker.

In Section 3 of the red team report, Known Issues, the investigators described the presence of known issues with the Sequoia Voting System. Sequoia notes that these lists are unvalidated and that when given thorough investigation by a jurisdiction, are found to lack merit and point, not to the equipment or software, but to errors by poll workers, issues brought about by distrust of the voting system or non-system related events.

Section 3.1 of the red team report, the Alameda County California Report is discussed. The Alameda county investigators recognized that any vulnerabilities identified could be and are mitigated by procedural mechanisms as intended by the system. As such, they conclude that Sequoia electronic voting system is inherently secure. A few items copied by the red team report deserve comment.

Item 1. WinEDS and other services use non-encrypted test passwords when communicating. The current federal certified version of WinEDS 3.1.74 does encrypt all passwords. Furthermore, the version of WinEDS currently undergoing federal certification is 4.0.0 has a completely new security access model, which strictly controls access, passwords and the database itself at both the application and database levels.

Item 2, the Edge uses constant hashes and DES encryption keys as allowed by current voting system standards. The portion of the system security scheme is in compliance with the required level of security. The risk of exploited -- the risk of exploit is mitigated by restricting access to the machines in all areas, warehouse storage, preparation and use.

The version of the Sequoia system, which is being targeted for certification under the 2005 Voting System Standards will implement a PKI methodology utilizing asymmetric key pairs and digital signatures for further improved security.

Item 3, using cryptographic techniques will not prevent the results being copied across results media, but will both prevent the results from being read and allow the results to be verified. The current approach is allowed by the current Voting System Standard and therefore is compliant with the required level of security. Any risk is mitigated by restricting access to the machines and the voting cartridges in all areas, warehouse storage, preparation and use.

The version of the Sequoia system, which is being targeted for certification under the 2005 Voting Systems Standards will implement a PKI methodology using asymmetric key pairs and digital signatures for further improved security.

Item 4, the WinEDS system uses Windows and therefore inherits the vulnerabilities associated with the operating system. As with most complex software systems, a common commercial off-the-shelf operating system is utilized. In this case, Microsoft Windows. The risk associated with attacking vulnerabilities in the Windows operating system are mitigated with common procedural methods. Sequoia also recommends that the WinEDS server and clients are not on an isolated -- are on an isolated network in a physically secured area.

Even with the precautions, it is possible for malicious software to finds its way back to the network via results cartridges or other mobile data storage devices that may be used with computers on a network. This is mitigated by insuring a strict anti-virus, anti-spyware, regime included are the most recent updates utilized in the functions included in the software that's enabled.

In section 3.2 of the red team report, Multiple Vote Attacks, the investigator notes what has become known as the yellow button attack. This is the attack the voter must reach around to the rear of the voting machine, pass the privacy panel, find and actuate in a specific pattern to the yellow button in the rear of the machine without the notice of any poll worker.

This attack is easily prevented by several means. The first is to disable the activation of the yellow button through a configuration setting in WinEDS, the election management system.

Secondly, numerous physical security measures can stop this attack placing the voting machine to the rear of the machine facing the poll workers aids in voter privacy to ensure that the surreptitious attempts to repeat activations through the yellow button will easily be seen. Jurisdictions can also place a physical seal over the button to prevent it from being pressed, until authorized poll workers remove the seal, using the prescribed change of custody procedures, and press the button.

The attack outlined in Section 4.1 and 4.2 of the red team report are examples of ones that require unfettered access to the machines for a long period of time, in a laboratory environment, is extremely unlikely that anyone would be able to develop such an exploit when typical security measures are taken to restrict access to the machines.

In many jurisdictions units are stored in secure controlled areas, where access to the units are controlled via electronic pass and access and movements recorded by close captioned TV.

In Section 4.3 of the red team report, Accuracy Testing Mode Detection. The investigators could determine if a voting machine was in test mode or in election day mode. This is not surprising and it is true of any system that provides a test mode of any sort. This opportunity to attack the system has been anticipated by both the vendor community and governments for many years and is the reason for parallel testing as required by the State of California. Parallel testing disables this attack and the State of California employs an excellent parallel testing program, which serves as a model to election jurisdictions throughout the country.

Section 4.8. of the red team report, Security of The MS SQL server, points to the need for personnel security by the customer jurisdictions. As is true with any election system, whether touch screen or paper based, some individuals have access to tally data. Persons with access to the central count server should undergo background checks, commensurate with the valuable data that they maintain. Windows audit logging must be enabled, the allowable log size maximized, and the log secure against accidental or intentional alterations or deletions. All of these practices are detailed in ISO 27001, ISO 17799 as described in the introduction of this document.

Section 4.10 of the red team report, Possible Unsafe OS Choices, indicates the recommendation for use of Windows 98 or ME for client computers. This is due to the age of WinEDS 3.1.012 currently certified in the State of California. Newer federally certified WinEDS packages and their documentation call for Windows 2000 or XP with their enhanced security policies.

Section 4.11 of the red team report, Physical Security, indicates that tamper evident seals are easily bypassed. While seals can be removed, as is their intended use, they cannot be removed undetectably. In cases where poll worker access is required to fulfill election responsibilities, tamper evident seals provide a convenient method to bring to the surface any attacks on the equipment so that the equipment can be quarantined and the election continue without its results becoming suspect. Tamper evident seals have been used in the military environment for many decades, and consist of adhesive tapes with unique identifiers, which cannot be removed without breaking them. They could be placed on every access point, including access covers, the chassis screws and a record kept of the numbers. Jurisdiction procedures will log the unique identifiers on the tamper evident seals match established records to ensure that no equipment tampering had occurred.

Section 4.13 of the red team Report, Forging Update Cards and Voter Cards, is mitigated through physically securing the voting machines, election specific information on the voter card, and traditional and current poll worker training. This scenario requires the attackers gain access to the voting machines and could successfully extract and utilize the information regarding voter card programming.

Not only this static information needs to be extracted, but the ballot style for a particular precinct would need to be known to the attacker in advance. Without valid ballot style information, which changes from election to election, this attack fails, if the voter card is rejected by the voting machine as invalid. Poll workers are responsible for ensuring that only voters that have just received voter cards from them approach the machines. It is unreasonable to believe that a person or persons could approach the line of voting machines in a precinct without having been credentialed, and especially that an attacker or group of attackers could do so repeatedly.

Section 5, Attack Scenarios, while these attacks may have been successful given the uncontrolled environment of the investigation, they would not succeed in an actual election.

Attack Scenario 1, insert a malicious HAAT USB stick into the initialization process, relies on two assumptions: That there is a pool of HAAT USB sticks for initialization, such that a malicious HAAT USB stick could be inserted into that pool; and autorun on the WinEDS computer is allowed. The HAAT USB sticks are specific to each precinct or polling location, thus it would be extremely unlikely that a malicious USB stick could be inserted into the jurisdiction's HAAT initialization process. As stated above, autorun features should be disabled on all computers performing election-related tasks.

Likewise, the assumption that a large number of voters do not check their vote on the paper record, when it scrolls in front of them, providing both visual and audible cues as to its existence, and when the voter is forced to interact with the voting machine to produce the record, is also false.

Sequoia always recommends that the WinEDS server and clients are on an isolated network in a physically secure area with strict access control. All mobile data storage devices should be checked for viruses and spyware on a stand-alone computer before being introduced to the secure area. The U3 flash drives should not be permitted in the secure area and should never be used on the system.

Even with these precautions, it is possible for malicious software to find its way into the network via results cartridges or other mobile data storage devices that may be used with the computers on the network. This is mitigated by ensuring a strict virus and spyware detection regime is implemented on the system, including ensuring the most recent updates are utilized

Attack Scenario 2, the same as Attack Scenario 1, but with a fleeing voter that did not review their paper ballot, is likewise implausible. How would the malicious software know that the voter had actually fled? The interaction with the voter and the poll worker is the same regardless of which one actually completes the ballot casting process. Poll workers need to keep the voting machines open, so fleeing voters' ballots are typically cast quickly after the voter leaves the voting machine, so time intervals would not aid the malicious software for determining when it could successfully change a voter's ballot choices.

Attack Scenarios 3 and 4 rely on the voter leaving the voting machine within a few seconds of the voting process ending, and the next voter not appearing at the machine long enough for the voting machine to print and obscure its VVPAT record. This is not plausible in the least. Voters, some carrying purses, children, and other items, will take several seconds to leave the booth, during which time any number of them would notice the odd behavior of the voting machine, and that it voided their VVPAT record.

Some voters will leave the booth quickly. If the voter leaves the booth quickly, then the next voter is likely to see the voided paper record and either notify the previous voter or call a poll worker. Either of these actions calls attention to the errant machine behavior. And Edge VVPAT requires ten or more seconds to print a VVPAT page, so there is more than adequate time for voters to read the maliciously voided record and be alerted to the machine behavior.

Attack Scenario 5 is easily thwarted with tamper evident seals and the scope of effort required to tamper with a statistically significant number of Edge units. It is implausible to successfully carry out this attack.

Attack Scenario 6 regarding voter cards would require that attackers gain access to the voting machines and could successfully extract and utilize the information regarding voter card programming. The attacker also needs to determine the ballot style information that is valid at a particular precinct/polling location. If the card is programmed with no style information or incorrect style information the card will be rejected by the voting machine as invalid.

Assuming an attack of this nature was attempted, poll workers are responsible for ensuring that only voters that have just received voter cards from them approach the machines. They will notice if a person or persons enter multiple times and/or approach the machines without having received a voter card from them. Polling places are set up so that the voter must pass through a credentialing station prior to obtaining a voter card, and thus prior to approaching the voting machines.

Traditional and current poll worker training and Election Day actions would prevent voters from voting multiple times. Voter cards are embossed with jurisdiction or Sequoia Voting Systems specific artwork so that volume purchases of blank voters cards could not be used successfully in an attack unless they were also forged with the jurisdiction's artwork.

Attack Scenario 7 regarding access to WinEDS and installation of malicious software fails with simple mitigations. Sequoia always recommends that the WinEDS server and clients are on an isolated network in a physically secure area with strict access control. Full MS-SQL security should be implemented, including encryption of passwords, and a strict and secure password management regime utilized.

The possibility of malicious software having found its way onto the network can be further mitigated by ensuring a strict anti-virus and anti-spyware regime is implemented on the system. This includes ensuring the most recent updates from Microsoft are tested then applied.

This type of attack is mitigated if, as described in the scenario, WinEDS is loaded on the server before each election is initialized, and just before the Election Day. Further protection can be gained by taking digital signatures of the server after WinEDS installation and comparing them to hash values taken on Election Night. Procedures for loading software through trusted processes are published and practiced throughout various jurisdictions, as well as industries outside of elections.

Even in the extremely unlikely event that this sort of attack is attempted, the mitigations already discussed in relation to scenarios 1 through 4 would apply.

Potential Attack Scenario 8 regarding use of access to the 400C Central Count Optical Scanner to attack the tabulation of scanned ballots is also easily mitigated through the use of tamper evident seals. Sealing the compartment containing, the 400C computer would allow for rapid detection of this attack, which could then be thwarted completely by re-installing the software on the 400C through a trusted processes. Standard physical security practices, such as electronic passes and surveillance, would allow for identification of the attacker.

And my conclusion.

While this evaluation has been an interesting and helpful theoretical exercise, it did not represent a security risk analysis, and as such does not measure the severity of the actual threats in any meaningful way. The evaluation was limited to malicious tests, studies and analysis performed in a laboratory environment by computer security experts with unfettered access to the machines and software over several weeks. None of the traditional, statutory or recommended security procedures were in place. This situation is unrealistic.

Sequoia concludes that none of the threats outlined represent a realistic threat if the normal, procedural mitigations are in effect. We are, however, entering a few system vulnerabilities found into our ISO 27001 Compliant Corrective and Preventive Action System to further reduce opportunities for attackers.

We are also considering the broader implications of each attack to refine our established recommendations to customers regarding system security. Jurisdictions should consider conducting thorough security risk evaluations based on ISO 15804, Common Criteria for Information Technology Security Evaluation and/or ISO/IEC 17799:2005; and adopting security processes conforming to these international standards.

Lastly, the versions of the hardware, firmware and software systems evaluated were developed several years ago. While it cannot be guaranteed that all of the extremely improbable vulnerabilities identified are prevented by subsequent product development and updates, many are specifically addressed.

Sequoia also believes that this evaluation identifies some potential weaknesses in the current Voting System Standards, which have been addressed in later standards, and, as such, should the State believe that some of these threats outlined in the report are credible, it should consider purchasing new machines or updating to existing units that meet the 2005 Voting System Standards, and subsequently adopt the 2007 Voting System Standards when available.

On behalf of Sequoia Voting Systems, I would like to again thank the Secretary of State and her staff for allowing Sequoia to participate in today's public hearing and comment on the red team and accessibility reports. We look forward to working with Secretary Bowen, her staff and our customers this week and in the future as we go forward in providing secure, accurate and accessible election equipment for California voters.

Thank you very much.

MODERATOR PÉREZ: Thank you.

(Applause.)

MODERATOR PÉREZ: Any questions for Mr. Bennett?

PANEL MEMBER FINLEY: You referred just now and earlier in your remarks to upgraded versions of WinEDS, the central election management server software for the Sequoia system. And I'd just like to clarify, you referred to one version that had been federally certified and another that was in the federal certification process. Are either of those versions certified by the State of California and are either of them in use by any of your 21 county clients?

MR. BENNETT: I do not think I can answer that at this time.

PANEL MEMBER FINLEY: Can you answer whether a system that hasn't been federally certified can be used in California?

MR. BENNETT: The system that went through the top to bottom is currently certified in the State of California.

PANEL MEMBER FINLEY: I'm asking about the later versions that you identified as having enhanced security features?

MR. BENNETT: I can tell you that the most recent federally certified version that we complete will be the version that we bring to California for certification in the future. As you know, rank choice voting and other features will be part of that process.

PANEL MEMBER FINLEY: So the answer to my question is no?

MR. BENNETT: The answer is I don't think I can accurately answer your question at this time. But in further discussions, we can get back to that.

PANEL MEMBER FINLEY: You stated in your statement that one of the attacks was based on a false assumption, that voters will not check the VVPAT printout of their votes before casting their electronic ballot. Do I understand that right?

MR. BENNETT: I believe that's part of this statement.

PANEL MEMBER FINLEY: Okay. Are you familiar with a video tape that was made of the first use of the Sequoia VVPAT in the State of Nevada, I believe, in 2004?

MR. BENNETT: I'm familiar that there were video tapes of that, yes.

PANEL MEMBER FINLEY: And are you familiar that -- are you aware that elections officials here in California took the position that that video tape demonstrated that a significant number of voters did not look at the VVPAT?

MR. BENNETT: I'm not aware.

PANEL MEMBER FINLEY: Okay. Thank you.

MODERATOR PÉREZ: Any other questions for Mr. Bennett from the panel?

Thank you, Mr. Bennett.

MR. BENNETT: Thank you very much. And a copy of the statement is available on line on our website for those that need it as well as Business Wire.

MODERATOR PÉREZ: Very good. I want to thank everybody in the audience for your incredible patience. You know at times I saw some head nodding and some head shaking. That's a completely appropriate response. I want thank everybody for being very mindful not to interrupt with any verbal or audible responses that would have delayed our proceedings. And I know this is an important topic that people want to be heard on.

What we're going to do now is we're going to take a 30-minute break. We're going to reconvene at a quarter to 1:00. We're going to reconvene at 12:45. At that time, I'm going to open up the public hearing for everybody in the room. If you want to be heard, if you want to speak during the public comment hearing, make sure you fill out a card. If you've already filled one out, drop it off at the check-in table before you go to lunch or drop it off as soon as you come back. While this room is ADA compliant, access to the podium in the front can be difficult. If you have difficulty in getting to the front podium, just let us know, we'll bring the microphone to you.

We have a sign that will go up indicating when people have 30 seconds and when their time is up. If you need audible cues indicating a limitation on your time, please let us know as well and we'll accommodate that. But, again, I want to thank everybody for their cooperation throughout the morning and I look forward to hearing everybody's comments when we reconvene at 12:45.

Thank you very much.

(Thereupon a lunch break was taken.)

AFTERNOON SESSION

MODERATOR PÉREZ: Good afternoon. I want to welcome you all back to the hearing of the top to bottom review. I want to thank everybody for their cooperation during the morning as we went through the main portion of the prepared discussion.

Now, we're in the public comment period of the hearing and I'd like to remind anybody who wants to speak, but hasn't filled out a speaker's card yet to please do so and turn it in at the table outside of the auditorium. I'll announce the order of speakers 2 to 3 people in advance, so please be prepared to speak when the person in front of you concludes their remarks.

We've taken some liberties in structuring the public comments section to make sure that we don't have folks from, for example, one organization all grouped together and stuck at the end. So when you filled out your card, the order in which you turned it in is not directly the order in which you'll speak. So I wanted to draw your attention to that.

Each speaker is limited to 3 minutes. In some instances, as per our rules, a few people ceded their time to somebody else, so we've put together those cards of individuals who ceded their time with the individual to whom they ceded their time. And in no case can anybody have a total allocation of time more than 9 minutes.

So that we can accommodate everyone who wishes to speak, I encourage people to not be repetitive. If someone has already made the comments you were intending to make, you may simply want to give your name and associate yourself with their remarks. That will help ensure that people with new ideas and comments have the opportunity to address us as well.

While speakers are more than welcome to pose questions that they hope the Secretary will consider over the next week, I don't want people to have an expectation that there will be direct responses to those questions. The panel will not be responding to any questions that are posed, but the questions that you raise will be taken into consideration as the Secretary takes action over the next week.

I want to remind everyone that any comments you make here today and any comments that you submit in writing are part of the public record and will be disclosed to anyone who makes a Public Records Act request. As mentioned at the outset of the hearing, this hearing is being webcast, video taped and is being carried live via conference call.

Once more, this is a public hearing not a debate and I want to remind and encourage everyone to continue to act in the respectful manner in which we've all comported ourselves this morning.

With that, we'll begin the public comment portion of today's program. The first 3 people to come forward will be Philip Harlan, Eve Roberson and Stuart Schy. And I apologize if I've mispronounced any of the names.

So if Philip Harlan if you'd please come forward.

MR. HARLAN: Hello. Am I coming through on the microphone?

MODERATOR PÉREZ: Yes.

MR. HARLAN: I'm Philip Harlan. I live in Healdsburg, California, Sonoma County. And I'm blind and I'm also a little bit of a computer -- I play around with computers a lot and I think I understand a little bit about technology and I'm worried about security. So I know you people are worried about security and I heard the comments from the gentleman from the University of California, and I heard the comments from the vendors. And I understand that they have opposing views probably based on where they come from and where they get their finances.

And I don't get my finances from anybody that's connected with voting. I'm only interested in preserving or -- well, let's say preserving our democracy. And so as a blind man, I know that there's going to be some blind groups here that do not care as much about security as they do whether or not I got to market the ballot because I'm blind. And I want to just say that my major concern is security and I'm not just worried about security of hackers from the outside, but I'm concerned about security from people on the inside who might have a specific interest in having a specific candidate win an election. If you think elections are not worth stealing, you're living in a different word than I do.

So I just want to say to this panel that when you're considering all this, remember that it's more important that we -- at least from point of view, it's more important that our votes are counted correctly than whether I cast one on an absentee ballot or on a machine or if I had assistance.

Thank you.

MODERATOR PÉREZ: Thank you very much. Next we've Eve Roberson followed by Stewart Schy and then followed by Steve Weir.

MS. ROBERSON: Yes, Mr. Chair and members of the Board, I'm Eve Roberson from Santa Rosa, California. I'm a former California election administrator for 15 years. And so I do understand the concerns of the registrars of voters today that these very expensive computerized voting machines that they have purchased in good faith may not be approved for use in your elections next year and is legitimate concern.

However, the reason these voting machines cannot be approved obviously is that many computer experts have carefully examined them and have testified to how easy it is to hack them and to change the vote. It's clear that these touch screen machines were sold to the registrars of voters of our counties based upon the false representations that these devices were protected from hacking and that they could be used for the purpose for which they are intended, in other words to record honestly the votes that a cast upon them. However, it's been demonstrated over and over again that these statements by the vendors were simply not true and that they would or should have known that their machines were never safe from hacking.

Therefore as a former election administrator and as a California taxpayer, I believe firmly that the registrars of voters have the right and the duty to return these defective voting machines to the vendors and to demand a full refund of the purchase price.

(Applause.)

MODERATOR PÉREZ: And again if -- and I appreciate folks wanting to express their support or opposition to a statement, but I again want to remind you, as the day wears on, that practice will wear on, so we need to make sure that we don't do any audible demonstrations of support or opposition. And I want hold that against your time.

MS. ROBERSON: Thank you. Non-computerized, affordable voting machines have recently become available that have well been received by the voters with disabilities. And there's still time before the next election to obtain these machines for persons with disabilities and also to provide paper ballots for all voters. The optical scan machines could still be available to count the votes of these paper ballots. Our democracy depends upon open and fair elections. Paper ballots are the only way to guarantee that. We've learned that the hard way.

So I'd urge the Secretary of State to ban these corrupted computerized voting machines from use in any election to be held within the State of California.

Thank you.

MODERATOR PÉREZ: Thank you.

Next we have Stewart Schy followed by Steve Weir and then Candy Lopez. And, sir, you didn't put your mailing address on the card, so if you'd please give us just your city of residence.

MR. SCHY: Santa Rosa.

MODERATOR PÉREZ: Thank you.

MR. SCHY: Thank you, Secretary Bowen and the panel for doing as much needed top to bottom review of electronic voting systems in California. I'm a retired electronics engineer and computer consultant with over 20 years experience working with people in the disability community. Since 2006, I've been a volunteer member of the Sonoma County Logic and Accuracy Panel. Sonoma County uses ink marked ballots centrally counted on high-speed optical scanners. Using HAVA funds the county initially purchases Hart Intercivic eSlate equipment and installed one eSlate in each of 350 precincts.

I was disturbed to note that in the 2006 primary only 166 disabled voters used the eSlate machines. In the November 2006 election, 225 votes were cast on these machines. And a quick calculation dividing the money spent by the number of votes cast came to about $18,000 per ballot cast on the eSlates. In comparison, the independence provided by a power wheelchair is about $15,000

Last February, because of this concern and acting on my own, I sent a letter to each of the 58 registrars of voters in California to ask how effective their new HAVA equipment was in serving voters with disabilities. To date, I have received 27 replies. Those counties that used HAVA funds to add equipment to their existing systems showed very similar results to those we got in Sonoma county.

For those counties who completely replaced their systems using HAVA funds, I cannot determine what the usage was for voters with disabilities. I believe that HAVA did not mandate the purchase of electronic voting equipment, but enabled the option of approved devices as a way to meet the needs of people with disabilities.

My study is still in incomplete and it lacks official sanction, but it indicates that we need a more in-depth inquiry into how helpful the HAVA program has been to disabled citizens in California.

I do want to thank those registrars and county clerks who answered my survey letter and would hope that more would follow suit.

Thank you.

MODERATOR PÉREZ: Thank you.

Now, we have Steve Weir followed by Candy Lopez. Mr. Weir has 9 minutes as 2 other people have ceded time to him.

MR. WEIR: Mr. Chairman, ladies and gentlemen, thank you. I'm president of the California Association of Clerks And Elections Officials. And this is a very important issue for us today as it is for everyone in this

State. But I did just simply want to ask the registrars and their staff if they would stand up. Many do not want to speak today, but wanted to show their presence.

Thank you very much.

I was truly excited when Secretary Bowen met with myself and my executive board on the 10th of January of this year. And she indicated her desire to do a top to bottom review and I was supportive of that. At that meeting we were 17 months away from a Presidential primary and I indicated to the Secretary I thought we had perhaps just enough time to pull this off and to do so in a manner that wasn't disruptive. And, of course, you all know, as the Secretary has said, the rest of the story. Within a matter of days there was discussion of an early primary. And within 2 weeks a bill was passed, the rules were waived and we now have an early primary. So we lost the opportunity to do a methodical process. But nonetheless, we've offered our willingness to participate in this process and for whatever reason have been excluded.

I do support independent review of voting systems including source code. And I support the legitimate real-world penetration testing as part of that certification. I'm sorry that I found the top to bottom review to be more about headlines than about definitive science or the pursuit of legitimate public policy.

We have been told that no malicious code has been found in the source code. We've also been told that that wasn't even the target of this operation. Given the public debate nationally about the vulnerability of source codes, if it is true that the source code was not reviewed and that looking for malicious code was not part of this process, we have both missed an opportunity and perhaps created, what I would consider to be, a public policy blunder.

In all honesty, California registrars have expected and California voters deserve a definitive answer to the question, is there malicious code in our voting systems in California? This process could have yielded that answer. That part of the debate could have been over. We missed it.

Equally troubling to me is the lack of published clear, sound and testable standards for the penetration portion of this study. Matt Bishop stated in his communications with ACM in March of '07, where he titled Fixing federal Evoting Standards Concerning the Testers the following quote, "These are the testers. They need the computer science communities help to achieve engagement in writing clear, sound and testable standards." That didn't happen here.

Incidentally, part of the original document that was put forward about this process quoted the NIST, the National Institute of Science and Technology's, recommendation that penetration studies be part of the certification testing. But it also went on to say that there needs to be published standards before you can do those tests. If clear, sound and testable standards are not forthcoming from this effort, this too will be another lost opportunity and a public policy blunder.

Lastly, the choice to test voting systems in the theoretical laboratory setting without even considering the real world circumstances has deprived us, yourselves, the testers and the public from knowing what the real-world issues are concerning these voting systems.

In the real world California has the toughest voting standards requirements and testing in the nation. For electronic voting, which is used in over half the counties in California, we require the production of a voter verifiable paper audit trail. Every manual audit of this paper trail documented against machine totals has shown that the systems have reported the votes accurately.

The Secretary of State and former Secretaries of State have mandated and conducted additional checks against electronic voting. This is called parallel monitoring. The Secretary of State has published the results of several tests and has concluded in every case that the machines have quote, "accurately recorded all the votes cast on those machines. "

While I consider the materials presented to be a theoretical hologram, that is to say an image of what could be, this has happened without the mitigation that everyone freely admits was ignored during this process.

This is what I consider the materials not to be. They are not a comprehensive top to bottom review. They lack published standards. They lack a key examination under real-world circumstances. And, for whatever reason, they lack the involvement of the registrar of voters in the State of California who also represent over 100,000 of our citizen poll workers that we rely upon to conduct these elections.

There is not one piece of evidence here that any voter in any election has had their vote compromised. There is no smoking gun here. The question of the legitimate use of the voting systems in California is now clearly before the Secretary of State.

I have 5 questions I hope that the Secretary would consider in making her review:

Are there any factual inaccuracies in these materials?

Do any systems procedures or county policies follow prohibited or vulnerable practices?

Do existing security procedures and policies mitigate any identified threats? And, if not, are there policies that can be readily implemented?

4th, are there any good ideas in these materials, which, by the way, I think there are, that haven't been thought of and can they be incorporated into standards?

And then lastly, based on the materials presented, is there anything that would warrant a drastic action by this Secretary of State to radically change voting systems and to do so in the next week?

I am very concerned that these materials have been released without the presenting of obvious and legitimate answers to proposed threats. Matt Bishop stated, and he was again one of the leaders in the recent publication from March, the following: "The moral is that one can never verify that a voting system has no flaws even if all the source code is available. Perfect voting systems do not exist. The goal is to build voting systems that are as good as possible. These goals involve policies and procedure as well as software assurance. Unless they are taken into account, reviewing only software may give a misleading idea of the security of the system."

I propose to you today that that very fact has happened here today. California registrars want to emphasize that we stand ready and willing to participate in this process and we're ready and willing to look at our internal and external processes for improvement.

With that, I thank you for your time. I appreciate the time that was ceded to me and the courtesy that the audience has shown to us.

MODERATOR PÉREZ: Thank you very much.

Next, we have Candy Lopez followed by Greg Taber and Cathy Darling.

MS. LOPEZ: I'm Candy Lopez. I'm the Assistant County Registrar in Contra Costa County. I've worked in county election departments since 1972, assisting in the planning, conduct and certification of federal, State and local elections. I have learned that no single step in an election exists independent of other steps. They are tied together in an intricate process layer upon layer.

When components are examined, they should be examined in the light of related processes and dependencies. Because the voting system review did not take into consideration election processes and security procedures currently being used by the counties, the public has been left with the false impression that undetected tampering is possible in an actual election.

A template of questions regarding security practices was developed by prior Secretary administrations in order to assist the counties in making sure that critical security procedures were in place.

Last week, the Secretary's staff requested information on each county's security plan, which caused me to wonder why the plans previously filed by the counties had not been included in the early review process. However, after reading the reviewed comments, I believe the State's template does not cover the full range of processes the counties do have in place.

For example, nothing in the template requests information on logic and accuracy testing practices. According to the red team's summary, what the security policies and procedures should be and how they should be implemented, including best practices, is a matter that lies with the acknowledge and experience of state's elections officials.

The Voting Systems Subcommittee of the California Association of Clerks And Election Officials was organized to create a regular forum for dialogue between the State and the counties on important issues surrounding voting systems and their certification. To me, this subcommittee is the appropriate group to develop a guiding document.

The head of the voting systems division in prior secretary administrations actively participated with the clerks and election officials on this subcommittee. The person currently holding that position has failed to attend, even though monthly invitations have been extended requesting his participation. I hope that will change.

As we move forward to analyze issues raised in the review and work to establish minimum standards for security plans, assuring that those issues which can be mitigated through procedures have been addressed.

Thank you.

MODERATOR PÉREZ: Thank you very much.

And I want to just draw everybody's attention, we have a timer here at the main podium, so if you'd keep your eye up there at the time as your speaking.

Our next 3 speakers are Greg Taber, Cathy Darling and Alan Dechert.

MR. TABER: Good afternoon, distinguished panel and audience. My name is Greg Taber. I served on a local election observer panel in the early nineties. I'm a civil engineer and I've lived in Riverside County all my life.

Please decertify the Sequoia Voting System used by our county. In condemning this review a vendor was quoted in the newspaper quote, "When used in conjunction with proper security procedures and protocols, our voting solutions ensure that every vote is safe, secure and accurate," unquote. Mr. Bennett echoed this sentiment today.

As the red team report correctly points out, quote, "Policies and procedures that look effective on paper may be implemented poorly rendering them ineffective," unquote. We cannot rely on the election worker's integrity as a primary safeguard in the system. The recent conviction of 2 Cuyahoga County Ohio election workers proved the folly of that course.

I also have a personal experience that bears light on this concept. On February 8th, 2007 I was asked by local activists to help hem audit the paper receipts from the November 2006 election in Riverside County. These receipts are used when custody of the bag containing the cartridges and other precinct material is transferred between the precinct inspector and the collection station official. They are a vital link in the so-called chain of custody.

I was shocked. The number of instances where important information is missing from the receipts is truly disturbing. Many were unsigned. Some had discrepancies between the precinct and the collection center and the number of cartridges, meaning lost cartridges. Even more disheartening are instances where the collection persons apparently took it upon themselves to fill-in the missing information for the precinct worker.

But from what I can tell, there are wide disparities in the way staff followed the requirements. Twenty-one of the precincts in the second district had serious problems of counting the vote. Only 6 percent had the receipt completely filled out. Out of a set of 14 precincts in the first district, 11 weren't countersigned by the collections center worker. I've made copies of a couple of the receipts for your information.

Amazingly, the situation had not resulted in any disciplinary action by the registrar of voters or the Board of Supervisors. Actually, the registrar was lately lauded by the Board. Although, I don't know, maybe it was you're doing a heck of a job browning kind of thing.

(Laughter.)

MR. TABER: But clearly we can't put our sole faith in the integrity of the local officials. We must have an easily additive verification of the voters intent. The paper ballot is the simplest, most secure and most transparent way to accomplish this.

The authors of the report sagely claim the crucial question as quote, "Whether the election process taken as a whole meets the requirements of an election as defined by the body of politic," unquote. I believe the answer to that question is a resounding no.

To quote James Madison from Federalist Paper number 51 quote, "But what is government itself but the greatest of all reflections on human nature. If men were angels, no government would be necessary. If angels worked the government, either external or internal controls would be necessary," unquote.

Please don't depend on men acting like angels. Please decertify these machines.

Thank you.

MODERATOR PÉREZ: Thank you very much.

Our next speakers are Cathy Darling followed by Alan Dechert and Brent Turner.

MS. DARLING: Good Afternoon. Cathy Darling. I'm the elected county clerk and registrar of voter in Shasta county.

I am not going to talk to you about all the policies and procedures that we have in place to utilize the Sequoia voting machines that we use in my county because I believe some of my comrades or colleagues will be talking about that. And you have here in the Secretary of State's office all of that documentation already. I look forward to seeing the document review portion of the UC report, which we have not seen yet.

I did want to talk about a couple of things, mainly the fact that no election official either

California or from any other State are included in this review process. There are a number of examples where that may have been helpful, in particular, the accessibility report on page 18, there is a strap that's used to attach the accessibility keypad to the arm of a wheelchair for a voter that needs that.

The entire page 18 talks about where to put the accessibility pad. And if you hang it on the privacy screen where there's Velcro, then it might off all. And there's a sentence I wanted to read. "It appears that the Velcro cloth roll adapter on the back of the keypad supplied for testing is a new feature that has not been generally available on currently fielded Sequoia Edge systems in California."

Every accessibility keypad I have, which was delivered to me in June of 2003, fully 4 years ago, has that strap. Nowhere on this page does it talk about how to use that strap or how to make a voter who needs to use that keypad secure the keypad to the arm of the wheelchair in a way that makes it more stable for folks that have perhaps a sight impairment and also some mobility issues.

This is a very minor detail in this 155-page accessibility report, but it goes to show the lack of context in which some of these tests were performed.

I frequently use the analogy that conducting an election in my county is like holding a party for 90,000 people and everyone has to have their own personalized party favor. It's an incredibly complex task. It has 700 or 800 different individual tasks. We actually just document those about three months ago and I was blown away by how numerous they were. But having done it over and over, it's not that surprising.

My point here is that independent researchers from outside could have greatly benefited from some input from folks, as I said, even not from California, perhaps other state staff that use this equipment would have been of some assistance. But the fact that we've been cut our of this process from the very beginning leaves this report with some gaping holes and some glaring inaccuracies.

And I hope in the future that we can be included in this process to assist the Secretary in assuring California voters that their votes are secure. And my time is up.

Thank you.

MODERATOR PÉREZ: Thank you very much.

Alan Dechert followed by Brent Turner and Virginia Ontivaros.

And Mr. -- am I butchering your last name?

MR. DECHERT: Yes. It's Dechert.

MODERATOR PÉREZ: Dechert. Mr. Dechert has 9 minutes as well.

MR. DECHERT: I should be only about 5 minutes.

You have wrestled the patient to the operating table and cut her open. Diseased organs have been exposed. You cannot stop now. You cannot simply sew the patient back up and be done with it. Can you repair the organs with the instruments you have? Perhaps a few band-aids will work or perhaps one or more organs will have to be removed. You made the incision. You must tell us what you are going to do. You must decide. You must do it right.

The patient on your operating table is democracy herself. In February of last year at our behest, Senator Bowen held the first ever public hearing on open source software for elections. When people asked, what was the conclusion of the hearing, I have to say there was no conclusion. While some good information was heard and was generally positive for open source, no analysis was issued. The only bill in the State legislature relevant to this issue, AB 2097, died in the appropriations committee in May of last year.

At one point in the hearing Senator Bowen said disclosure to experts is a non-starter for me. One of the panelists from Accurate replied, it may be a non-starter for you, but it's going to be a non-starter for the vendors.

So here we are, we have disclosure to experts. At least 4 of our well-paid reviewers are experts from Accurate. Fine for them. Not fine for advocates of public disclosure. We want to know the details, and they say but we have just signed non-disclosure agreements to do this work. Advocates of full public disclosure are not satisfied with this. The public has a right to all the information about how the voting system works. I doubt the vendors are happy with this review either. You have a lot of unresolved unhappiness to deal with.

The vendors and the election officials say these are laboratory tests. These problems are not seen in the real world. Your expert reviewers say, it depends. Should we continue with a voting system that protects trade secret methods or should we move to a public system with no secrets. You need to decide. Maybe you already have enough information to decide. Maybe we need a new public hearing that will be conclusive on this question.

If the Secretary of State is going to proceed moving toward a public system, as she has indicated in the past, she needs to tell us exactly how she plans to get there. If she has a plan for this, that is a secret too, at this point.

He said. She said. We need to finish this operation. We are done with secrets. We need a solution.

Thank you.

MODERATOR PÉREZ: Thank you, Mr. Dechert.

We have Brent Turner followed by Virginia Ontivaros followed by Michael Covey, but I can't really tell from the writing.

Brent Turner.

MR. TURNER: My name is Brent Turner. I just handed in a document written by Jim March of Black Box Voting last night for your perusal. Mr. March is under the impression that this needs to take more of a criminal law approach. And that's cited in the paperwork there. The documentation that he's provided as has also already been tendered to the Federal Bureau of Investigation, as well as lot of local D.A.'s. And this is on the point that the Windows CE was inappropriate and there may be a consumer fraud issue. So we just wanted to bring that to your attention and I'll proceed with my statement.

My name is Brent Turner. I'm an activist for election reform and I belong to many groups. We appreciate the efforts of the great Secretary of State Bowen. The top to bottom results mirror the conclusions of previous scientific studies. We must now stipulate that proprietary systems are unsuitable for elections. Vendor and/or Microsoft interests can not be the barrier to transparency.

We request the State of California to move quickly towards hearings regarding paper ballot open source systems. Alan Dechert of Open Voting Consortium, who spoke in front of me, and Richard Johnson of Open Voting Solutions are at the ready to provide this service. And I know from speaking with Mr. Johnson back in New York, he's attempting to get certified in New York right now. And he's glad to do this work, basically, pro bono just to use California as a proving ground that these open source systems are at the ready and will be the quickest path to restoring voter confidence.

We have recently seen many counties and officials go towards open source. Recently some Presidential candidates have embraced the philosophy. And also our California State Democratic Committee has moved towards approving an open source resolution and have actually approved that with these secret software systems.

Per Roy Saltman who is known as the father of the certification process, there is no way to tend to the fixes, so we're really being run in circles here by the vendors. What we are calling for is open source hearings and being allowed to provide information on the points that Mr. Dechert highlighted.

Now that we've confirmed the vulnerabilities, we must seek the solution. I know that many will demand hand counts. And I want to remind them that the open source community, the open voting community embraces the hand counters as it's part of the systems. Certainly, hand counts are preferable to secret machines, but we are trying to move in this open source direction.

Public confidence must be strengthened by transparency. Again, Mr. Dechert and the Open Voting Consortium have information that continues to be proven correct with every new study.

Again, we want to conclude by thanking the Secretary of State. She's been a great champion for transparency. We respectfully request she utilizes her inherent power to implement open voting. The Open Voting Solutions group is agreed to forgo profit and to provide solution to this crisis pro bono. This will provide a crucial aspect of the necessary solution.

Thanks to all of you for your attention to this matter.

Thank you.

MODERATOR PÉREZ: Thank you.

Now, we have Virginia Ontivaros followed by Michael -- and again I think the last name is Covey of NFBC. And then Emily Levy.

Virginia Ontivaros?

Okay. We'll come back to Ms. Ontivaros if she comes back into the room.

Michael Corey or Covey, NFBC?

Okay. Emily Levy.

MS. LEVY: Be right there.

MODERATOR PÉREZ: Emily Levy.

MS. LEVY: Coming.

MODERATOR PÉREZ: Thank you. Followed by Mark Keenberg and Dero Forslund.

MS. LEVY: I'm Emily Levy with the Brad Blog and Velvet Revolution. And I'm going to address my comments to Secretary Bowen and hope she gets an opportunity to hear them.

Thank you for your courage -- your strength and courage that has brought you to this moment. I fear that even after months of testing, there's still an elephant in the room that has not been tackled. Even if you and your staff could plug every hole in physical and software security and the voting systems were made fully compliant with the accessibility requirements of HAVA, it would still not be safe to use these systems.

Why not? Because even if they were absolutely protected from hacking, the systems, and therefore our elections, could still be rigged. There is no way to provide an absolute safeguard against electronic voting systems being delivered to the counties and presented to the voters already compromised. For this reason alone, these systems and others like them must never again be used in our elections.

The irresponsibility and lack of ethics of the vendors has been amply shown. They've misrepresented their products. They have installed uncertified software. They have cut corners in developing the security of their systems. And that's just the beginning of the list. Clearly, they are not guided by ethics or commitment to the public good. Clearly, they have other priorities.

Is it so unbelievable then that they might rig an election? We have a crisis in voter confidence that can only be solved by creating a true basis for voter confidence. Only transparency and public involvement can save our democracy now.

Perhaps more than any other human being in this country you, Secretary Bowen, are in a position to take bold decisive action that will reverberate around this nation and turn it in its tracks. The next step is to decertify these machines, to send these vendors packing, and tell them not to come back, not with another promise, not with another model and not with another role of toilet paper. The people of California, the People of the United States and frankly the people of the world are depending on you to do this.

Thank you.

MODERATOR PÉREZ: Thank you.

Next, we have Mark Keenberg followed by Dero Forslund and Tim McNamara.

MR. KEENBERG: Yes. My name is Mark Keenberg. I'm the co-founder of the California Election Protection Network. I'm from Oxnard, California.

MODERATOR PÉREZ: And Mr. Keenberg has 9 minutes.

MR. KEENBERG: I don't think I'll use them all.

One of the things a lot of the ROVs say they've had incidents with problems with electronic voting. I think that can be solved with mandated record keeping by the Secretary of State's Office. I believe that the Secretary of State's Office should have mandate incident report forms available at every voting polling site. They should be numbered in sequence. And they should be in 3 parts. One part goes to the voter. One part goes to the ROV. And one part goes to the Secretary of State's Office. And these should be posted within 36 hours after the voting, then we could really see if there's really problems with these machines. I think that would solve a big issue and it would clear up a lot of -- give a lot transparency to the use of these machines.

When Kevin Shelley was Secretary of State he decertified the Diebold TSx machine because he found the software in the machine did not match the software that was in escrow. Now this was probably the first and only time there was a comparison made between the escrow -- the software in escrow and the actual software in the machines on voting day.

I'm going to make a comparison, and a lot of people are going to laugh at this. And it's a model for testing that is done in car racing, NASCAR in particular. And a lot of people are going to say well what does racing have to do with elections. They're very similar.

There's a lot of cheating in both. In car racing there's an old saying, if you ain't cheating, you ain't trying. And the same thing can be applied to elections. And I think we see it. We've seen it since 2000 with electronic voting machines.

In car racing, a car is presented for tech inspection before they go out and qualify and they're inspected when the race is over. And there's been a lot of publicity this year about cheating and crew chiefs being suspended and massive fines. And we've also seen cheating the Tour de France with very intensive testing.

Well, I think we can use the same role in testing electronic voting machines. And I think that every central tabulator before the election day starts, they should go in and they should burn a copy of the hard drive of all the memory and every card that goes into the machine during the day and when the election is over. I think the same thing should be done with electronic equipment at every polling site, and that is really impossible to do. And I think that that's a good enough reason, if you can't burn a copy of the hard drives of the memories and every card that goes into every DRE and every PVR unit that's used in every polling site in the State, and if we can't do that, we have no tech inspection. We have no race day, election day tech inspection and we don't know what's in those machines.

And I think they should be eliminated. And if you eliminate that, you can use paper ballots. HAVA states that if you don't have direct electronic recording at the polling site of their hand-marked ballots, you don't need to scan for over and under voting. And you eliminate the PVR DRE units, you don't have to scan for over and under-voting. This would eliminate all the electronic devices at a polling site.

If people are wondering what they're going to do with all these devices that we're not going to use anymore, I'm in the scrap metal business --

(Laughter.)

MR. KEENBERG: -- and I'm willing to pay 5 cents a pound for every electronic voting device in the state. We've got trucks standing by. We'll come pick them up.

And I guarantee I'll send them to China.

Thank you.

(Laughter.)

MODERATOR PÉREZ: Thank you, Mr. Keenberg. Next we have Dero Forslund.

MR. FORSLUND: Good afternoon. Dero Forslund, Clerk/Recorder/Assessor of Trinity County, Registrar of Voters.

We're using optical scan systems along with TSx units. The TSx units that we're using are the third variety of touch screens. We've been actually having them in place since about 1999. When we went with the optical scan because of surprisingly -- concerns we had about computer systems back then, something called Y2K. And as you may recall, there was a lot of concerns with computer systems, what's going to be effective and failed at that point. It turned out to be not the case.

Actually I am pleased to see that these reviews are being done. I am somewhat disheartened by the fact that they didn't really review what we do in our office, because that's where I felt I needed the help.

The other thing -- and I'll touch about that a little more -- but one of the things that I was concerned about relative to the executive summaries on at least a couple of the reports indicated that the reviewers thought that giving more time, we might find more vulnerabilities. I'm a little afraid that we'll go through the process of figuring what to do here and then come back later and find out that we're going to be doing it again. So I'm concerned that a little more time might have been more appropriate here.

I understand the issues with respect to the time. I have elections coming up in November in my county, so I'm going to be needing to use this equipment with -- and we're sitting here not sure what we're going to have available to us actually.

Professor Bishop -- and I tried to write down, but I'm not sure that I got his quote exactly right. But I think this is the gist of what he was saying, is that policies and procedures should be a part -- considered a part of the system. And without considering those as part of the system, I don't know that we've really done what needs to be done. When the equipment that we have now was put in service and certified by the Secretary of State's Office, they said you can use it as long as you follow these particular policies and procedures. I think we should be looking at those policies and procedures to see whether or not they truly do mitigate vulnerabilities that have been found.

And some of them I think probably we'll find out aren't sufficient. One of the things I think is kind of ironic is that the VVPAT that we put on all of our touch screens right now is really a mitigation measure for concerns about being able to verify what somebody voted. But now we find out in accessibility reports that, gee, the VVPAT doesn't work very well for the disabled, which is the reasonable why we have the touch screen in the first place. So I mean that's an example of what happens when we don't really look at how the mitigation is applied in this way.

So I think -- I just think we need a lot more work to be done. You know, I'm all in favor of doing everything we can to find out that these systems are active and as good as they can be. But I don't think we're far enough along to really know how to answer it. I don't know what the answer is, but I'm really concerned.

Thank you.

MODERATOR PÉREZ: Thank you.

Now we have Tim McNamara, followed by Conny McCormack, followed by Deborah Seiler.

MR. McNAMARA: Hello. My name is Tim McNamara from Los Angeles County where I'm Assistant Registrar with -- over the Election Services Bureau.

The Bureau recruits and trains over 26,000 poll workers and opens 5,000 poll places for major elections, among other functions.

I've been working in local election offices for 16 years in various capacities and have chaired the Voting System Subcommittee referenced earlier by Candy Lopez and co-chair of the Voters with Specific Needs Subcommittee. In those capacities, I've worked with election officials, academics, and others interested in elections at the local, state, and national level regarding vulnerabilities to voting systems and voting system implementation, including those involving all paper ballot systems.

Many of these folks have been concerned about studies and speculation about voting systems that don't rank threats regarding their likelihood of being manifested vis-a-vis destroying voter confidence.

I have significant experience in implementing voting systems at the county level, most importantly related to getting poll workers ready to use new equipment, and have seen very bad things happen related to hasty last-minute mandates from non-local entities related to voting systems.

I'm here today to quickly address just a couple of notions in support of the comments of CACO President Steve Weir and other county election officials. There are plenty of examples of trying something new on a large or small scale leading up to a major election that have been extremely problematic or dramatically harmful regarding voter impact, including impact on voter confidence. And, by the way, this review is quite possibly one of those actions given the terrifying headlines that have appeared over the past few days related to it.

The only hero on the seen will be the folks that deliberate and address any probable threats -- probable threats that may likely come to fruition and in an extremely objective way vis-a-vis the proximity of the untried election landscape now upon us; that is, the fall elections this year and three state elections next year, which you know we've never tried before, and the fact that by all evidence elections in California have been conducted in a rational fashion and under the current technology.

Decisions made that unnecessarily complicate the present election landscape will most likely have dire consequences, and those complications will be traceable to their roots. With this in mind, please rank the threats and bring the mechanical experts as soon as possible into the picture, that is, the local election officials, to get you as much needed help regarding those threats that are truly threats that need to be addressed in this precarious environment.

To feed off Mr. Bishop's analogy, the SOS could do very well by taking on a longstanding offer by county election officials to meet with them, they who are the real equivalent of the local police in his analogy.

By the way, to play on the SOS Bowen's opening analogy, many members of my family including myself have been roofers. And giving that, I know many of my fellow election officials have made good metaphorical roofers in addressing the real issues behind the red team reports and will serve the SOS well in addressing them further to build voter confidence instead of tearing it down.

Thank you.

MODERATOR PÉREZ: Thank you.

Now we have Conny McCormack, followed by Deborah Seiler, followed by Dennis Floyd.

MS. McCORMACK: Good afternoon, members of the Panel.

And, John, I don't know whether -- Mr. Perez, I don't know whether you mentioned some folks have ceded some other time.

MODERATOR PÉREZ: Yes, I'm sorry. Thank you for drawing my attention. Ms. McCormack has nine minutes.

MS. McCORMACK: I'll try to do it as quickly as I can. But I'll try to not use up the nine minutes.

Thank you.

MODERATOR PÉREZ: Thank you.

MS. McCORMACK: First of all I'd like to introduce myself. I am the Registrar/Record/County Clerk in Los Angeles County. I've held that position for a little over 11 years. But prior to that, I was the Registrar in San Diego, and prior to that in Dallas, Texas. So I stand here with 26 years of experience as a local election official, and I've been involved in overseeing the counting of more than -- I can't even tell you -- tens of millions of ballots. And I certainly know the complexities of all the different kinds of voting systems, from lever machines I started in Dallas, at the punch cards, to optical scan, and to DRE. So we do have the experience. And I do echo our President Steve Weir's comments that we are available for consultation.

Computers, both at the central tally level and at the precinct level, have been successfully tabulating ballots for many years, more than 40 years, in a real world environment. And we've already heard folks say how important it is to have a real world environment with the procedures. And that this report that has come out has, and I quote, said, "It is done in the absence of procedural mitigation strategies."

So I really think that's very important, and I think it needs to be key for the Secretary's considerations.

I won't repeat some of the quotes that have been mentioned before, with Mr. Matt Bishop's article from March of 2007, in which he himself said that policies and procedures had to be taken into account in order to have a legitimate process.

But I will quote on from that article, which goes on to say that against -- and it asks the question: "Against what threats should the system be protected?" And I think that goes to a little bit about what Tim McNamara was just saying.

There was not in his report any type of a hierarchy of threats or any kind of threat scenarios presented in a way that you could determine what the practicality or the possibility of these threats were.

One of the threats talking about a voter going into a polling place with a common office tool and what -- there was no assessment of the likelihood of that occurring or what poll workers might do should such a nefarious voter try to break into a piece of voting equipment.

More disturbing to me also is that there was comparative analysis with may other types of equipment, such as paper ballots, and the ease of ballot box stuffing that does have historical evidence in our country and in other countries. And in addition to attempted fraud in that respect also has been involved in just mishandling of ballots where some -- ballots have completely disappeared or are getting misplaced, because handling paper is very difficult in the electoral process.

Senator Bowen stated in her opening remarks that this morning the counties may have security procedures in place to address the identified vulnerabilities, but she doesn't know if we do.

Back in January I had suggested that the detailed security plans that all the counties put together prior to last November's election, which were required by the Secretary of State, I had suggested to then Election Director Caren Daniels-Meade that those be studied by the Secretary and their findings shared with the counties so that we could all learn from best practices. And that was many months ago, back in the early winter.

However, we never heard anything back from any of that. And so I find it rather odd now that there's an indication the state doesn't know what the counties do, because I know our plan was over a hundred pages that we submitted. It was extremely detailed.

I'd like to continue by providing a little bit of an historical perspective, and maybe even a little humor.

I think we're all lacking a little of that right now. And when I was reading Saturday's L.A. Times and, you know, there's an article that came out about the Secretary's review, it struck me how very similar it sounded to an article that appeared in the Los Angeles Times, October 8th, 1969, almost 38 years ago, in which the headline read "How Elections can be Rigged via Computers." And this is the article. And it starts by: "Admirals and generals have their war games, computer experts have their own form of intellectual exercise. And recently such computer experts in Westwood broke into and worked on breaking into election computers and the possibility of this happening in the real world."

And the article, you can read it, and you swear it would be dated this week. It is absolutely the same article. I enter it into the record for both historical interest and perhaps a little humor. I don't think I have to enter the L.A. Times from Saturday. I think you've all probably read it.

So I think that it is important for us to realize that we have confronted and have dealt with what these computer problems potentially could be in elections for many, many years and we do have processes. And we also -- as historical practices, that we have not seen these computers being broken into. So I think it's important to mention that.

But most important, I think that all of us want to do -- and I know Steve Weir mentioned it and I think your next speaker's going to actually give you some points because I've seen some things she's going to say. But we really need and all of you need, and I know you know you need, is sort of move forward and -- several of the speakers have said, "What are we going to do now?" So moving forward is really important.

And I think it's important that in Washington right now, both at the House of Representatives and at the U.S. Senate, there are two bills that are very active, HR 811 and S 1487, that would mandate two of the things that we're already doing in California, which is the paper trails nationally and the manual auditing. And so I think that, you know, California's had a pretty good track record in having this process already very election-reform oriented.

In addition to contracting with the UC to do their review, the Secretary also last month established a working group on post-election auditing. And last month that working group, chaired by Mr. David Jefferson, called me and asked for some input -- and I appreciated that call -- and he asked for some specific input: What is the manual auditing process like in L.A.? How much does it cost? What does it involve? And I was very pleased to of course be asked and, second of all, for solid data. And we provided to them on January -- to that committee -- working group on July 19th, this document I entered into the record.

The gist of it is that in Los Angeles -- and I know it's been going around in the whole state for about a quarter of the state, so you could sort of take these numbers and probably times them by 4 -- the manual one percent audit we do to check randomly to see whether or not the computer's counting accurately. That audit we've been doing for about 40 years. In L.A. in November '06 entailed counting 25,526 ballots from 88 precincts, which ended up being 1.7 percent of our precincts' ballots. As to the 52 contests on that ballot, the actual number of votes tallied in order to compare and verify the vote results in each contest with a computerized count entailed painstakingly hand counting between a half a million and a million votes, depending on how many selections each voter either made or skipped. This labor-intensive manual tallying comparative process required a staff of 50 employees 10 hours a day, 7 days a week, from November 11th through certification of the election on November 27th.

The cost was $207,000 in our county. It did not entail absentee balloting. And since the Legislature has as of this year required that, so we have estimated that cost next year will be 73,000.

So that's somewhere around $280,000 just to do what we did last November. And the turnout was around 50 percent. It will probably be higher next year, so we'll have to count more ballots in those precincts.

So I think that some scale here is important.

The costs, if there's going to be -- this committee apparently is considering adding more manual tallying. And I said this definitely needs to be looked into, because we have a 40-year contract record of doing pretty well with this. And when we do find anomalies, and sometimes we do -- and we do this process publicly and transparently and we've had many voter activists in our office last November everyday. And I would have to say we had a very good feedback and very good -- they appreciated us being able to be there.

So should there be any increase in that, the Legislature would need to get involved because it is a law right now. And the Secretary has indicated that if she were to ask for more auditing like that, she would go to the Legislature.

So in closing, I'd like to reiterate what Dero mentioned a few moments ago, that we -- this whole process is really focused on next year, next February, and this one week timeframe and the reports being rushed. And we're having elections around the clock. I mean we've had congressional elections this year. And then we all have these November elections with many of the voters. So elections are continuing to go on with the same equipment we've been using and with a manual auditing proving the results.

So thank you very much for your time. I will leave this for you for the record.

MODERATOR PÉREZ: Thank you very much.

And if we can get some kind of -- let me just collect that.

Go ahead, Deborah. You have six minutes.

MS. SEILER: Thank you.

Good afternoon, ladies and gentlemen and members of the Panel. I'm the Registrar of Voters for San Diego County.

San Diego County has successfully run its past three elections using the Diebold touch screen system and its related optical scan system for absentee voting. We're proud to be fully HAVA compliant. And the system has proven to be 100 percent accurate in parallel monitoring conducted by the past two Secretaries of State, one Republican, one Democrat.

San Diego voters have expressed confidence in their voting system and their voting experience by returning surveys that have given us a rating 4.6 on a scale of 5.

Today we are 190 days from the February presidential primary election and an ongoing series of major statewide elections in 2008.

Yet we find ourselves at this critical juncture threatened with the loss of our voting system or severe and potentially fatal restrictions on its use.

I would like to remind the Panel of the dangers of rushing significantly new products or procedures into use without lengthy vetting, training, and backup planning.

It is well known that San Diego experienced problems in the March 2004 election when a card activation device had problems. It had an unknown battery issue that confused poll workers. Though it was easily remedied, many polls did not open on time.

Since then, we have worked hard to iron out these unknown and unintended consequences, and feel confident about the current status of our system.

We know we will also have to work to continue to improve. Indeed, continuous improvement is part of our motto. But we have many security measures in place, including the serially numbered, tamper-proof seals which are recorded. And we constantly seek enhancements in our operations.

We're concerned therefore about drawing extreme conclusions and actions based on studies that were billed as a top-to-bottom review was in fact not even close. There are currently nine voting systems actively used in the State, and only three were studied. That means a full 48 percent or almost half of the state's voters -- registered voters had either no components tested or only one or two components of their voting systems tested, leaving them uncertain about the potential vulnerability of the systems -- or system used in their county or city.

Given that the three systems reviewed were all found to have vulnerabilities, it can only stand to reason that the remaining six systems are likely to as well. Perhaps their vulnerabilities are even greater. But the point is, we simply don't know about the vulnerabilities of the systems that were not reviewed.

This means that if the Secretary chooses to decertify or severely restrict use of our system, we have only two available options. We either select an alternative that has no vulnerabilities or one which may have worse vulnerabilities but vulnerabilities that we cannot predict or fully mitigate against.

It is well known that election officials have security policies and procedures in place that were not considered as part of the red team attacks. The researchers had unfettered access to the hardware, the software, source codes, and passwords. They were allowed to load unauthorized software on to servers to tamper with results.

The relative security of systems including paper were not assessed, and accuracy and reliability were not part of the review. Election officials were not allowed to be a part of this process, and thus their real-world perspective and operational expertise were not accounted for in this process, which simply now amounts to a laboratory experiment.

Despite this, it is important to note that no malicious code was found during the reviews.

This entire exercise takes me back to July of 1986 when I was in the Secretary of State's Office as Chief of the Elections and Political Reform Division. At that time, New York Times reporter David Burnham in a front-page article quoted a Princeton researcher as alleging that the upcoming presidential elections could be rigged because so many counties use the ELAB source code that was applied by the old Vote-a-matic system.

Although the system had been used for 20 years with no incidence, such as those posited by the Princeton professor, the allegations and speculation were taken seriously.

My response at that time was to recommend legislation to deposit the source code into an escrow account and to expand the post-election audit of 1 percent or manual recount to ensure that it encompassed every single contest on the ballot. These I believe were measured responses that have served us well over the past two decades.

It is now my recommendation that the Secretary of State take an equally measured response in the absence of a complete review of all voting systems and the absence of finding any malicious code. I would urge the Secretary to demonstrate steady, even-handed leadership by first refraining from any precipitous action until all systems are reviewed and a full analysis of the issues, including mitigating security measures, accuracy, and reliability, are made a part of that review.

Second, to continue to conduct parallel monitoring and expand the program as necessary to include all voting systems.

Third, send Secretary of State staff to our offices to learn more about our real-world operations, work with us to understand the various methods we employ to secure our systems.

Fourth, expedite the certification of security upgrades which we know vendors have already developed in response to these security studies.

Fifth, avoid a piecemeal approach to our election systems that could have the unintended consequences of not causing counties to stumble in the 2008 elections. Do not force us to jump from the proverbial frying pan of the known to the fire of the unknown, untested and unperfected.

I stand ready to work with the Secretary of State.

Thank you.

MODERATOR PÉREZ: Thank you.

Now it's Dennic Floyd, followed by Dan Kysor, followed by Julie Bustamante.

MR. FLOYD: Good afternoon. My name is Dennis Floyd. I'm with San Diego County. And while most of the year I spend being a lawyer for the County of San Diego, for the context of the next three minutes I want you to think of me of me in my alter ego of what I do on every election day, which is go into the poll as a volunteer and either help run the poll or work in a couple of polls keeping the polls open and going. My experience there is very practical and it's the day-to-day, how-to-get-things-done sort of job, something I haven't heard really dealt with today at all.

I was especially concerned to hear Professor Bishop talk about how little time he had. And it was unfortunate that he didn't have the benefit of even a minorly seasoned poll worker to assist him as he was going through the scenarios with the Diebold touch screens. The four attack scenarios he described would have been used. Any poll worker with even one election under their belt. And they could have explained to him that these issues are extremely loud, the printers are loud, the card inject system is loud. And no one -- no poll worker would sit there and listen to the machine clacking away or the cards being ejected over and over with the same person standing at the machine and not had taken action and done something about it. I guess that would have been the blue team that would have assisted the red team in their evaluation. It is Unfortunate they didn't have the time to do that.

And as a poll worker, I'm concerned with the outcome of these proceedings, because I see either one of two scenarious: Either the systems are going to be decertified, in which case the poll workers recognize there won't be a system to vote on. What we'd be left with is -- in some people's mind is a hand-marked paper ballot that will be hand-counted by, guess who, the poll workers at the polling place after they've spent 15 hours working the polling facility. And some people may think that's an easy function. But the State of New Hampshire did a study on hand counting paper ballots and determined it would take at least six seconds per contest to conduct a hand-count of ballots. In California we generally have 10, 15, 20 contests on each ballot. They're very complicated. And multiply that times a standard precinct with 200 or 300 ballots, you've got three and a half to four hours of hand-counting. And you've sent your retirees and your moms with kids at home home from the polling place after midnight. And of course the ability to do that count is going to be affected by the fatigue that they felt after all those hours at the polling place.

Then of course the results are taken to the polling place -- or to the central count where they have to be entered. So hand count is not an option.

Conversely, we're concerned that restrictions will be imposed that will make it practically -- or impossible to comply. We hope that when the Secretary considers any options other than letting machines continue to do as we've been trained for the last year, that she weigh in her mind the poll workers and the impact that these procedures that she will create will have on those workers.

Thank you.

MODERATOR PÉREZ: Thank you.

Next we have Dan Kyser, followed by Julie Bustamante, followed by Dave MacDonald.

MR. KYSER: This microphone's kind of low, but that's okay.

Good afternoon, Madam Secretary and members of the Election Systems Review Board. I am the Governmental Affairs Director for the California Council of the Blind, where we have long advocated for voting systems that are accessible, usable, and private for all persons with disabilities and especially those who are blind or visually impaired.

The right for a private, independent, and verifiable method of voting must not be sacrificed in the attempt to resolve the outstanding issues with respect to direct voting equipment DREs machines.

The criteria listed for the certification, although sweeping in scope, fails to consider the existing civil rights of current voters with disabilities. Since much expense to the taxpayers and time and effort by counties has been expended, we recommend certification of all current machines' status for a period of time -- these would be for Hart, Diebold, and Sequoia and the other systems -- to meet the accessibility criteria -- and the criteria we believe was accurately listed in the top-down report -- setting a timeline for meeting benchmarks. By doing this, you allow the industry to solve some technical issues. Which really, if you think about it, you know, no one's doing research on VVPAT direct access for blind and visually impaired individuals. You know, we've been claiming, as Secretary Bowen knows, we've been claiming that we did not have direct access to VVPATs from the screen. You have the access to the computer but not the screen. Where is the research in that? Why can't the University of California research that. Instead of this woulda, shoulda, coulda science, we could have actually been looking at a statewide research project to solve some of the problems that the industry cannot meet.

So a timeline benchmark approach is the prudent way and we strongly urge the Secretary to adopt this.

Thank you.

MODERATOR PÉREZ: Thank you very much.

MR. KYSER: And I do have -- Mr. Chair, I do have official testimony.

MODERATOR PÉREZ: Perfect. We'll get that from you in just one second.

MR. KYSER: Okay. Thank you.

MODERATOR PÉREZ: Thank you very much.

Now we have Julie Bustamante, followed by Dave

MacDonald and Julie Rodewald.

MS. BUSTAMANTE: Thank you for this opportunity to be able -- to address the panel. My name's Julie Bustamante. I'm the Lassen County Clerk/Recorder and Registrar of Voters.

As you can see by the number of election officials who are attending this hearing today, we take our jobs very seriously. You will not find a more dedicated, hard working group of public servants. In the ten years that I have worked in elections, I've been truly impressed with the level of honesty, integrity, and efficiency that my colleagues demonstrate.

No matter how hard the job gets, no matter what legislation is thrown at us, we always get the job done, and we'll do it again.

Every county in California was required to file a procedure and security plan with the Secretary of State before the November 2006 election. I'm sure that if you thoroughly review these plans, you will find that most of the issues raised in the top-to-bottom review have already been mitigated.

HAVA requires that we have accessible voting equipment in every polling location. The Secretary of State insisted that we meet that requirement in the year 2006. And millions of dollars in HAVA money, federal money, was spent to do just that. Please don't throw the baby out with the bath water.

Thank you.

MODERATOR PÉREZ: Thank you.

Dave MacDonald, followed by Julie Rodewald, followed by Terry Hansen.

MR. MacDONALD: Good afternoon. I'm Dave MacDonald. I've been the Chief Information Officer in Alameda County for over 20 years. I've also been the Registrar of Voters for the last year and a half. So I think I bring a little bit different perspective to this than perhaps some others, since most of my career has been in implementing technology and managing technology; and I've been intimately involved with elections now for the last year and a half.

I think it's been acknowledged over and over again, this study has been done in a very sterile laboratory environment. There was -- as of Mr. Bishop -- Professor Bishop acknowledged, there was not enough time to do the study correctly. I think this is too important to rush through it.

I notice Mr. Finley is using a laptop computer. And I suspect -- I'm not sure, but I suspect that has an anti-virus software installed on it. If you give me that computer and let me take the anti-virus software off of it, I suspect I could introduce a virus. Therefore, going to the logical conclusion, I don't think you should use that laptop. Put it away. It's been compromised -- it can be compromised.

Professor Bishop also talked about layers of security, defense in-depth. Let me just describe in Alameda County how we'd accomplish that for one of our processes.

We have a vote count room where we have our server with a vote tally software. To gain physical access to that room you have to go through several locked doors with special combinations. You then have to go through another door that requires a physical key to unlock it. Very few people have the key to that room. I don't have a key to that room. You then have to know the alarm code to disable the alarm.

So now let's say you get through all that layer -- those layers of security, you gain access to the room. You come to our server cabinet, which is a little bit bigger than this podium, a little taller. It's got a special key on it. We've changed the key to a unique key only for Alameda County. And now you get into the network. And we keep talking about the network.

The network exists inside that box. It's a wire basically just a few feet long. It is not connected to what many people think of the network as the Internet. It does not exist. For you to plug in a laptop into that server would require, first of all get through all the layers of the security, get in and do it -- now, this is going to be the propeller heads in the audience. We've got port level security that's defined by the Mac address. You cannot plug into that computer -- into the server and get in. It can't happen.

What do we do to make sure that the registrar of voters staff can't do that? Well, we have a separation of duties. We've got the IT Department who doesn't have access to that room, they can modify it. In other words they can plug into the server. But the ROV staff can't do it.

So we've -- I think we've implemented many of the things that Professor Bishop talked about. And I would really encourage this process to go forward. And take into account the kinds of things that counties have implemented to mitigate the vulnerabilities.

Thank you.

MODERATOR PÉREZ: Thank you.

Julie Rodewald, followed by Terry Hansen and Kelsey Ramage.

MS. RODEWALD: Good afternoon. Julie Rodewald, County Clerk/Recorder for San Luis Obispo County. I've been elected Registrar of Voters since 1994 in that county.

I'll just make two brief points. And many of my fellow registrars have made similar points before me. Obviously we all have security procedures in place in our office. Three minutes is not enough time to detail all of those. And, frankly, I was disappointed that the review did not include review of those mitigation efforts that we undertake, because I think it would have been a valuable lesson and experience for all of us.

You've heard everybody including the researchers say that there was not enough time for this study. And I think we're all aware of the old adage that a job worth doing is worth doing well. The recommendations that your Panel makes, the decisions that the Secretary of State will make this week are going to have far-reaching effects for elections in California.

This is an important job, safeguarding our democracy, our elections, I certainly hold near and dear to my heart, as do many of the people in this room, hopefully all the people in this room and all of our voters. Let's do this job well. Partner with the Secretary of State and the local elections officials and the security vendors. Let's review and revise our procedures if they need to be revised. Let's get those in place so that we can continue to ensure the accuracy of our elections, not only in 2008, but for years to come.

Thank you.

MODERATOR PÉREZ: Thank you.

Terry Hansen, followed by Kelsey Ramage, followed by Ann Barnett.

MS. HANSEN: Good afternoon. My name is Terry Hansen. I'm the elected Clerk/Recorder/Registrar of Voters in Yuba County.

And Mr. Runyan and Mr. Tobias on page 44 of their assessability report most acutely identified the dynamics of the relationship in which we find ourselves. And I quote, "As a technology driven by the needs of public policy, voting technologies are subject to political as well as technological and economic storms. The best way to weather those storms is to build trusting collaborations among manufacturers, public officials, experts, advocates, and testers in a manner that is open to the public and communicated clearly."

As you know, a voting system is comprised not only of hardware and software components, but procedural security measures must be evaluated and should be considered as a part of this system.

The executive summary provided by the Secretary of State identifies scenarios that could occur with unlimited access and unfettered -- unlimited time and unfettered access. This is one component.

The election officials have successfully developed and implemented security procedures and policies to prevent this unfettered access, as proven with years of actual uncompromised elections in California. This is component 2.

Mr. Runyan, Mr. Tobias, and their team have provided invaluable insight to vendors and election officials to further advance federal HAVA compliance for citizens with disabilities. This is component 3.

It is the sum of these parts that equates to integrity, accuracy, and sensitivity to the voters and the election process in California. It would be a great disservice to the citizens of California and potentially the entire country to undermine the confidence of the voters with a rush to judgment by way of a study without one of the components necessary for a balanced conclusion, that being the input of experienced election officials.

This top-to-bottom review, at best, should be used as a first step and not a final conclusion.

In closing, I would remind you credibility and trust does not come from chaos.

Thank you.

MODERATOR PÉREZ: Thank you.

Kelsey Ramage, followed by Ann Barnett and Bev Ross.

MS. RAMAGE: Hello. I'm Kelsey Ramage from Santa Cruz.

MODERATOR PÉREZ: You have six minutes.

MS. RAMAGE: Actually there was some limit -- I think I just have three minutes, but there was --

MODERATOR PÉREZ: Gail Work, she ceded time to you, or is she keeping time for herself?

MS. RAMAGE: I was going to give it to her because I wasn't going to be here. But then I'm here. So I'll keep it very brief. Then perhaps she can --

MODERATOR PÉREZ: Okay. We'll give you three minutes and then we'll insert Gail Work immediately after you then.

MS. RAMAGE: I'm a citizen who reads a lot about voter safety, and I check on issues around the country regularly online. And I'm horrified what's happened to our voting systems. And the credibility is shot in this country. People no longer think that the votes count.

I understand that the registrars are working very hard to have good systems. However, the companies are compromised and the machines are compromised. This review shows that any capable hacker can break into it and change it. And we know those who can, will. And I know that registrars may wish to apologize for what -- that they wish to apologize the fact they already have these intact systems. But the systems are around machines which are untrustworthy. And if we cannot our vote, we do not have stability in our country.

We're watching everything change radically. We must know that our votes count.

And perhaps someone has said this. I don't think so. It was said by a very famous person. "It matters not who casts the vote, only who counts the vote" - Joseph Stalin.

Thank you.

MODERATOR PÉREZ: Thank you.

To correct the error then, we have Gail Work, then Ann Barnett, then Bev Ross.

MS. WORK: Hello. I'm Gail Work, and I'm the volunteer chair of the Election Integrity Committee for San Mateo County Democratic Central Committee.

And first I want to commend Secretary Bowen and her staff for her thorough and courageous review of the voting systems. This is long overdue, and we have great interest in the results.

The many broad categories of voting machine vulnerabilities identified by the review make it very clear that these machines are not good enough for our democracy.

The voters are tired of all the problems that have surfaced across the country. The problems in Ohio and Florida; vote flipping; overvotes; disappearing undervotes such as in Sarasota, Florida, in November of 2006. The voters are tired of new software versions that are supposed to patch up security for our elections. Clearly these systems have serious security vulnerabilities that require increased oversight from our Secretary of State.

So why have so many voters become worried about the elections in California?

We've seen partisan appointed registrars with their photos in vendor marketing materials. This cozy relationship with vendors is questionable at best for public servants. We've seen in San Diego election results that are certified prior to the votes being counted. We've seen sleepovers where electronic voting machines are sent home with poll workers for sometimes weeks at a time, breaking any chain of custody. And if we can't provide custody for these machines, we shouldn't be using them.

The arrogance shown by some registrars indicates a lack of attention to the voters' concerns. We need much higher manual audits to bring the statistical reliability of audits to 99 percent. We need greater chain-of-custody security.

Public observers need greater access, to have more eyes on the elections process. In addition, the Elections Code needs to be enforced and strengthened.

The voters deserve complete assurance that every vote is counted as cast.

For the record, I'd like to add the issue of cost and fiscal accountability to this hearing. These very expensive privately controlled voting systems are depleting our county budgets. In some cases nationally maintenance costs have run as high as 1,000 percent over initial estimates. Our local county services are already overburdened, and these machines will continue to drain local coffers.

We cannot afford the fiscal drain and lack of security these systems represent.

This democracy belongs to citizens and the voters of California. It is not for sale.

And I thank Deborah Bowen for your public service and your integrity.

Thank you.

MODERATOR PÉREZ: Thank you.

Now, Ann Barnett, followed by Bev Ross and Ana Acton.

MS. BARNETT: I'm Ann Barnett, the Kern County

Auditor/Controller/County Clerk/Registrar of Voters.

I applaud the Secretary of State for her efforts to identify vulnerabilities in our voting systems, because all of us certainly want to eliminate or mitigate any vulnerabilities that we have.

But we do have a bit of a Catch 22 today. First, we're having hearings on reports to which both vendor and registrar should respond. But the detail we need in order to do an adequate job in responding hasn't been released, and rightfully so. So in reality, neither vendor nor county official can adequately respond to the public.

Second, we now have identified vulnerabilities without an assessment of risk, which the red team readily agrees. But without assessment of risk, we have details for political posturing and eliciting emotional responses, but little practical value without the assessment of risk.

As an auditor as part of an audit I am required to perform a risk assesssment. In doing so, I identify -- I identify potential risk, I determine a level of probability. We evaluate mitigation measures, we determine risk, and then we determine audit procedures if any is needed to test that risk.

What we're doing -- what we're discussing today is Step 1. Four steps still remain.

For example, there's a risk of damaging the GEMS server via modem. If that modem isn't connected, the risk is very low.

Today's discussion is only one piece of the puzzle. We've been told personally by the Secretary and her staff that she really isn't afraid of happening by registrars and their staffs. Now that's good. And none of us are naive, because we really do have the ability to damage an election. However, we also have a lot of internal procedures to ensure our ability to detect and deflect such a disaster, none of which are covered in this report today.

We are not critical of the testing that has taken place. In fact, in a different timeframe, registrars could have expanded upon the findings for paper ballots as well. However, Secretary Bowen has stated, time is not our friend.

What I would like to do is put today in perspective. What we are doing is evaluating a very important but small piece of a big picture. The sad reality is that the remainder of the picture will get little or no press and will be mostly unknown to a public that has been dissolution by partial information.

Thank you.

MODERATOR PÉREZ: Thank you.

Now we have Bev Ross, followed by Ana Acton and

Dr. Judy Alter.

MS. ROSS: Good afternoon. My name is Beverly Ross. I am the Tehama County Clerk and Recorder/Registrar of Voters.

Tehama County's purchased a Sequoia AVC Edge 1 for -- and the optical scan system for use by our absentee voters in September of 2003 to replace the then noncompliant punch card voting system, DataVote, as required by HAVA.

All components of these systems including the 400C and WinEDS operating system were utilized successfully for the first time at the March 2004 primary election. With continued use and by adding the voter verified paper audit trail prior to the June 2006 primary, our voters are very pleased with this system's ease of use and are confident with the fact that their votes are counted accurately.

Our senior citizens as well as our voters with special needs have appreciated the fact that many of them can now cast their votes unassisted at our polling locations.

Tehama County has also successfully participated in parallel monitoring as required by the state on three separate occasions. As a smaller county with approximately 30,000 registered voters, this has been a huge investment for our county. I hope that Secretary Bowen would not take any actions that could cause further financial burden to counties such as Tehama, who have very limited financial resources.

The top-to-bottom review tests were not conducted in a real election world scenario. You have left out any and all of the mitigating procedures that would prevent such attacks. Therefore, it is crucial that you review the security procedures and policies that have been developed and those that are being brought forward as a result of this study.

I would ask that you work with the vendors and those of us that are actually in the trenches to develop any new procedures from this point forward.

Please take the necessary steps to afford elections officials the opportunity to continue the preparation for the upcoming 2008 election cycle with the systems currently in use.

I do agree that after reviewing the documents provided as of this date, I have obtained information that could be utilized to improve the manner in which we further secure our equipment, our facility, and our operations.

You will not find a group more dedicated to doing their job to ensure voter confidence in the election process than California elected officials and their staff members with the continued support of our vendors.

Thank you.

MODERATOR PÉREZ: Thank you.

Ana Acton, followed Dr. Judy Alter and Gail Pellerin.

MS. ACTON: Hello. Can you hear me?

MODERATOR PÉREZ: Yes.

MS. ACTON: All right. My name's Ana Acton from FREED Center for Independent Living.

And I'd just like to start by saying that we do not recommend decertification based on the results of the accessibility testing. It's been common knowledge that any of the certified voter systems out there do not provide perfect accessibility to people with all types of disabilities, but they do provide much greater accessibility than any previous voting methods that have been used in the past. And by decertifying them would be a step backwards and accessibility for people with disabilities to be able to vote independently and privately.

We support both state and federal testing for accessibility. We believe that's a really good idea, and with the end of hoping to continue with research and development of these systems to increase their accessibility for future models that are developed.

We also support the mitigation items that were laid out in the accessibility report that gives some mitigation for near-term elections. There are a lot of things that we could do that will help increase accessibility. But, like I said, the system we do have provide much greater accessibility for voters with different types of disabilities.

I'd like to also recommend that all accessible voting solutions that come to California, whether it be electronic, non-electronic, a ballot marking device, DRE, should all go through accessibility testing. At this point the AutoMARK, for example, has not gone through this accessibility testing and it should, just as any other non-electronic solutions that might be proposed.

This would give us a better idea. Right now we're just comparing electronic to electronic. And, you know, we don't have a real comparison as how it would compare to other types of devices that are proposed to provide accessibility to voters with disabilities.

Also, I'd like to recommend that voters with cognitive disabilities would be part of the voting process in the future. There's only two, I believe, people who identify themselves as having cognitive disabilities. So there should be a wider range of disabilities represented in that testing.

And once again, we do not recommend decertifying based on the accessibility findings. We support continued research and development in moving forward with accessibility and not taking a step back.

Thank you.

MODERATOR PÉREZ: Thank you.

Dr. Judy Alter, followed by Gail Pellerin, and Freddie Oakley.

DR. ALTER: I'm Judy Alter, Director of Protect California Ballots.

I focused on the ES&S InkaVote plus precinct ballot counters and the audio device.

About 90 observers in L.A. County last November visited about 300 poll sites. They only reported on the observed problems. One-third of the 282 reports concerned the ES&S machines. About half of the reports, 81, where I studied revealed mechanical and software problems. Mechanical problems occurred in about two-thirds of the 38 poll sites. Some didn't work at all. They didn't turn on or they jammed, becoming inoperative. Two scanners worked intermittently after being fixed. Two replacements worked, two did not.

When poll workers could not replace the paper roll for error messages, they stopped using the scanner.

Because of these problems, if one scanner did not work, poll workers let all voters use the working one. Poll workers stacked completed ballots on the floor next to the inoperative scanners instead of putting them in the ballot box.

Almost 40 percent of these scanners also had software problems. They did not print out a zero tape. They rejected ballots with no overvote on them. Three scanners that first rejected then accepted the same ballot. Five rejected ballots printed "no error" messages. Because of these problems poll workers chose to override the error messages.

Problems with the seven ADA audio assist devices included poll workers not being able to set them up. Replacement devices didn't work after five tests.

One visually impaired voter spent a half hour voting on one. But the machine did not print out the voter's ballot. Five voters wanting language assistance voted with the help of their children on regular ballots instead of taking 30 minutes.

Registrar Conny McCormack told the poll workers that the InkaVote plus scanners were not tabulating votes. Twenty-one snap tally witnesses saw the poll workers print out the tally tape for the L.A. Times at Edison Exit Poll Reporters instead of counting -- hand counting the ballots as they did in June.

Finally, each scanner contains a modem. Observers cannot see if it's on or not. Current election cone bans, wireless capacity in DRE, but not scanners. We strongly recommend that you reconsider the use of these scanners based on this information and a complete report which I will submit with all the other reports.

Finally, I'm presenting 316 petitions with citizens requesting hand-counted paper ballots. We demand the Legislature stop allowing the use of secret vote counting on computerized and privatized machines. Please return to public accounted paper ballots, counted at the precincts, tabulated on adding machines with no software.

The mathematical process of adding numbers is not proprietary. Without ballots counted publicly, we don't have democratic elections.

MODERATOR PÉREZ: Thank you.

We have Gail Pellerin, followed by Freddie Oakley and Clark Moots.

MS. PELLERIN: Thank you, Moderator Perez, panelists, Secretary of State Bowen. My name's Gail Pellerin and I'm the County Clerk in Santa Cruz County. I do have some written testimony I'll go ahead and submit.

In an effort to be brief but riveting, I will go ahead and echo the sentiments of my colleagues that have spoken before me, particularly Steve Weir, Conny, Deborah, Tim, Kathy. I see all of you around here and I feel like we're all in the same boat together.

My colleagues and I are dedicated elections administrators who work countless hours to deliver safe and accurate elections for our voters. We conduct ourselves as nonpartisan caretakers of our democratic process, encouraging voters to register and vote, assisting voters who require help, and ensuring that every eligible vote is counted accurately.

We maintain transparent operations where the public is invited to observe our absentee ballot processing, testing of voting equipment, election night tallying, and of course the auditing of election day results.

We work with our voting system vendors and fellow users to continually improve the voting system and enhance the security. We are passionate about elections processes and the precious gift of voting.

I want every registered voter to vote. I always look for a hundred percent turnout in Santa Cruz County. And if you're not registered and you are eligible, I would like you to get registered and cast your vote. I feel very frustrated when I hear voters decide not to vote because they think their vote won't count.

I am confident in our Sequoia voting system that we use in Santa Cruz County that is primarily a paper base system with the one touch screen provides for accessible and verifiable voting. And I can guaranty that every eligible vote is counted accurately.

Recently our county grand jury conducted a review of our county's voting system. They invested nearly one year in their investigation. The jurors conducted hours of interviews, they came to our office, they looked at all of our security plans and all of our procedures. Their report, which was released this month, praises Santa Cruz County for our effectiveness in implementing the new federally mandated voting systme.

Moreover, it concluded that Santa Cruz County's voting system is fair, accurate, and secure.

I am proud and honored to be the Santa Cruz Clerk. I am especially proud of the elections team in Santa Cruz County that includes our full-time and part-time staff; college students; my county co-workers, many of whom leave their jobs on election day to help serve at the polls; our poor city clerks; and all of the poll workers who work tirelessly to ensure that voters have convenient access to voting on election day.

And I especially want to thank and am proud of our voters who refuse to stay home and not vote because of partisan politicians who want to leave the decision making to the few and the chosen.

Now more than ever we need to work together to develop a rational plan to continue to make improvements to ensure that California's voting system remains the best in the nation.

Thank you.

MODERATOR PÉREZ: Thank you.

Now we have Freddie Oakley, followed by Clark Moots and Philip Chantri.

MS. OAKLEY: Good afternoon. I'm Freddie Oakley. I'm the Clerk/Recorder of Yolo County, California. And I'm speaking on behalf of 90,000 voters in Yolo County, California, each one of whom I have spoken to -- among those I've spoken to has expressed support and gratitude for this top-to-bottom review. I hear a lot of people who didn't like this idea and don't like the way it was conducted. But not a single one of those is one of my voters.

I don't know if I've done a really good job of selling them on the need for scientific investigation or whether they're average voters in California who want to know that elections are being run in the best way possible.

What we've experienced in the last couple of months is sort of like an annual physical after you're 50.

(Laughter.)

MS. OAKLEY: You know, it's embarrassing and you're really anxious about it. You're worried about the process, you're worried about the results. And sometimes it's painful. But the results help you lead a better life. They let you know what's wrong. They tell you stuff you couldn't find out without an expert. And they let you make a plan to remediate your lousy lifestyle, your smoking of cigarettes, you're overweight. I mean that's what I hear every year.

(Laughter.)

MS. OAKLEY: So maybe I'm less anxious about this review than I would be if I weren't just such a wretched person altogether.

(Laughter.)

MS. OAKLEY: The good news is that now we know what's wrong to some extent, and we can make a plan to fix ourselves.

Now, I want to say that my biggest concern that's revealed in this -- I mean I had a very skeptical opinion of these systems anyway. I kind of thought they were junior college quality. And I'm not surprised to find out that there are some element of that in them.

But my major concern is the accessibility report.

And I'm truly shocked, I am truly shocked that, for instance, the legs on the booths aren't far enough apart. You know, they don't meet the minimum ADA standard for wheelchair users. And these are some physical problems that I think we need to very seriously consider and address.

You know, we bought these systems, many of us, primarily to accommodate voters with special needs and voters with disabilities. And I think we have let them down in the most appalling way. By, first of all, certifying these systems for use in California that have such obvious defects and then continuing to use them in spite of their obvious defects.

Now I think it's incumbent on us to take every action that we can to correct those, be it, you know, double sticky tape as suggested or putting divots on the buttons, whatever is necessary. And I really and truly hope that some serious consideration is given to that.

In conclusion, I thank you all very much for your hard work. I thank my fellow clerks for their hard work. And I truly thank the Secretary of State for going forward with this review under very difficult circumstances.

Thanks.

MODERATOR PÉREZ: Thank you.

Clark Moots, followed by Philip Chantri, and Jim

McCauley.

MR. MOOTS: Good afternoon, Mr. Chairman, Panel members. I'm Clark Moots, Director of Administrative Services of Placer County. I'm in charge with Information Technology for Placer County, and work with and support our County Clerk/Recorder/Registrar of Voters and his respected departmental IT staff.

Both myself and my staff have reviewed this initial report, and I would like to highlight a few key points contained within this report.

While Placer County utilizes Diebold, my comments pertain specifically to the overview of red team reports.

Contained within the executive summary, it is stated that each red team was to try to compromise the accuracy, security, and integrity of the voting systems without making assumptions about compensating controls or procedural mitigation measures that vendors, the Secretary of State, or individual counties may have adopted.

The report then goes on to state that in California, specific procedures for controlling access to the election systems and for setting up using and scoring the election systems is a local matter. If a problem is discovered, the people who know the law and election policies and procedures can modify their policies and procedures appropriately to attempt to address the problem.

And then under section 3 the report states that many but not all of the attack scenarios contained in these reports would be mitigated by fully addressing physical security, security training of staff, and contingency planning. The feasibility of developing policies and procedures that can be effectively implemented, what these policies and procedures should be, and how they should be implemented is a matter that lies within the knowledge and experience of election officers and the California Secretary of State.

And then under section 7 it states that judging the vulnerability of a system requires understanding both the nature and the implementation of the policies and procedures under which it is used. As the red team ignored compensating controls and mitigations, the raw counts of successful, unsuccessful, and untried attacks do not indicate which would still be successful in the face of compensating controls and how realistic these compensating controls would be.

In light of these statements within this report, I would encourage that the Secretary of State, prior to any decisions being made, work with each respective county on how their policies and procedure would mitigate the findings contained within these reports.

Thank you.

MODERATOR PÉREZ: Thank you.

Philip Chantri, followed by Jim McCauley, followed by Gloria Coutts.

MR. CHANTRI: Good afternoon. Thank you for the opportunity to speak today. My name is Philip Chantri, the Election Services Coordinator for Santa Clara County.

I'm happy to participate in any timely reviews that --

MODERATOR PÉREZ: If I may -- I'm sorry. I apologize. Please go forward. I thought I had additional time on you and I don't.

MR. CHANTRI: Okay. You can give me additional time if you'd like.

(Laughter.)

MODERATOR PÉREZ: Well, Placer has submitted quite a bit of time. Perhaps they'll cede some to you.

MR. CHANTRI: I'm happy to participate in any timely reviews that enhance the transparency and trust of the voting equipment for the voters of Santa Clara County. In fact, we were the first county to ask then Secretary of State Kevin Shelley of the ability to pilot a voter verifiable paper audit trail.

You know, I see a lot of long faces here today. And I think we all need to smile and breathe a sigh of relief and enjoyment. This is energizing to me. This is an opportunity to both show off what we do in my fine county, which I don't often get an opportunity to do, and to learn how to strengthen the numerous safeguards we already employ for our voters.

This report has and will over the coming days allow me to explain the numerous safeguards, procedural and otherwise, which we employ to negate the possibility of the attack scenarios that are written within. It will allow me to talk about cameras, badge access systems, stand-alone secured networks, alarms, seals, training, and numerous other things Santa Clara County has implemented.

Our voters have voted on over 5500 Edge 2 voting machines and eight 400C opical scan readers in a safe, secure, and reliable method since 2003.

In addition, it will allow us to look inward at ways to improve our systems through additional procedures and safeguards as we may deem necessary or may become required.

This is our democracy. And I am just as proud today -- no, I am in fact even prouder to be an election official working to implement that democracy for the voters of Santa Clara County.

We pride ourselves on having open and transparent procedures using our current voting system and welcome observations, questioning, and feedback from our voters.

We look forward to reviewing the source code and document review reports and participating in the process and providing additional feedback.

I am confident that in cooperation with our staff, voters, voting system vendors, and safeguards and procedures, we can continue to provide safe, reliable and secure elections to the voters of Santa Clara County.

Thank you.

MODERATOR PÉREZ: Thank you.

I now have Jim McCauley, followed by Gloria Coutts and Stephen Aye.

Now, Mr. McCauley, before you start, you have nine minutes. A couple of other people have ceded time to you. But our rules allow up to two people to cede time to any given individual. Folks from Placer County have some 22 cards, have ceded en masse 45 minutes worth of time to five different people. While it's completely consistent with our rules, I hope that we could get through it in less than 45 minutes between the five of you for whom time has been ceded.

MR. McCAULEY: I'm sure we will. I was hoping to speak last so I could tie it up. But I'll change my speech around.

MODERATOR PÉREZ: I'd be happy to have you speak last if --

MR. McCAULEY: Actually we'd move it quicker.

MODERATOR PÉREZ: Sure. Which of the Placer County individuals do you suggest goes first?

And I really do hope that we avoid going to 45 minutes combined.

But congratulations for reading our rules thoroughly and...

(Laughter.)

MS. COUTTS: I'm sure I will hold my time for three minutes.

My name is Gloria Coutts. I'm a citizen of Rocklin, Placer County; employee of the Placer County Clerk/Recorder/Elections Department. Thank you for the Secretary of State Bowen and you as members of this Panel and the interested members in the audience.

The key points I would like to make today is that the security of our voting systems must be considered in the context of prescribed and possibly needed policies and procedures that may be determined. Counties are responsible to follow the directives of the Secretary of State and of the certification requirements for the specific voting systems that they are using and for assuring that the policies and procedures are carried out for each and every election.

For Placer County, this amounted to over 300 separate items, which we have diligently reviewed item by item. And additionally we have procedures and security measures on top of that in numerous instances.

I would suggest that the reported vulnerabilities must be assessed in terms first of the appropriate mitigation measures already identified and established and any additional measures that might be recommended.

As many of the registrars have identified, the timeliness of this review and determination is quite critical.

I am certain that all of the California's registrars share in the goal of accurate and fair elections, and intend to work cooperatively with the Secretary of State.

And I would also in conclusion note that the policies and procedures that we are following for each voting system not only had been provided in a securities plan for each county before the election, but they also have been enumerated and presented to the Secretary most recently.

Thank you.

MODERATOR PÉREZ: Thank you very much.

Now I have several options for the --

MR. RONCO: Ryan Ronco?

MODERATOR PÉREZ: Very good.

MR. RONCO: The problem, Mr. Chair, is we thought you said that we could sell our time, not cede our time. So we brought a lot of people in the interest of being able to sell.

MODERATOR PÉREZ: Well, a couple of -- you know, Mr. Weir got some Placer time. Ms. McCormack got some Placer time. So congratulations.

MR. RONCO: Thank you very much.

My name is Ryan Ronco. I'm the Assistant Registrar/Recorder for Placer County.

We use the Diebold OS opical scan system as our primary voting system and Diebold TSx for our disabled voters for the HAVA requirements.

I appreciate the review that's being presented today, and I hope it makes us better as elections administrators.

However, I'm afraid that the report without discussing the security problems -- or, excuse me -- the security procedures counties put in place does not give the public a realistic picture of the security or possibly the lack of security of our systems.

It was discussed a little bit about procedures. And, yes, we do lay our procedures -- security procedures over security procedures. Is it difficult? Yes. Does it cause problems? Sometimes. However, we are sworn to protect and defend the Constitution of the State of California and the Constitution of the United States. And at least in our county, and I believe in all counties, we take that responsibility seriously.

While it may be beneficial to adopt or build security procedures as systems are developed, that is impossible in practice for every threat, as evidenced by what we are hearing here today.

Problems are found or legislation is passed and we have to adapt. Placer County's TSx bags are a real-world example of that. And I brought one of those for you. I'm not going to leave it with you. But I'd like to show you that these bags were developed with the TSx -- Diebold TSx in mind in order to be able to secure that TSx not only in a zippered bag but also with a locking seal that uses a tab, bar-coded, serialized number in order to be able to secure the zipper in place. This bag cannot be opened unless the tab on this bag is broken. And I think that these seals -- or a bag developed like this is the type of real-world example that would be able to fix some of the problems that some people had with sleepover issues, for example.

This is not mandated by the state. However, we went out and we found bags like this to be able to develop that -- develop a procedure to hopefully fix a problem. And so that's why we have bags like this.

I also don't think that you can underestimate the power of the public or our incredible poll workers as an important level of security we all use as a resource.

The report identified problems with locks, seals, software, hardware, firmware. However, keep in mind that an outside person intent on causing mischief would likely not be able to crack one of our multiple seals, bypass a lock, insert malicious code or otherwise hack into the system, reroute the system and reseal the device without being noticed by our polling place worker, whom in Placer County we hire specifically to assist voters with the use of the optical scanner on the TSx system.

As for an attack from outside the office -- or, excuse me -- from inside the office, we are lucky enough to have enough staffers to employ appropriate separations of duties. Plus the county has seven IT technicians in addition to 15 staffers. The technician responsible for programming our elections is not the same as the technician who oversees our office camera system or the person who programs our election -- or, excuse me -- a kind of card key access.

Because of this, it would take quite a cast of characters to affect an election. Is it possible? Yes.

But just like it was in the past, and will likely be in the future. But because of our dutiful staff, our interested public, including our Placer County Elections Advisory Committee -- who I'm glad to say I see a couple of those members here in the audience today -- we are getting better at security all the time.

I remain hopeful that this process will bring light to all of the important security procedures that are currently in place.

Thank you.

MODERATOR PÉREZ: I'm sure you get this all the time. But is that a Ronco device?

(Laughter.)

MR. RONCO: I wish that I had a little bit of a royalty on that.

Thank you very much.

MODERATOR PÉREZ:

MR. AYE: Hello. Stephen Aye. I'm a Senior Technology Analyst for Placer County Clerk/Recorder/Elections.

I wanted to speak.

MODERATOR PÉREZ: You have nine minutes.

MR. AYE: -- a little bit today on the top-to-bottom review in regards to Placer county, and to echo what most everyone else here has said that it is really impossible to accurately review the security of the elections equipment without taking into consideration the policies and procedures and current state laws that are set upon us in dealing with this equipment.

Placer County utilizes a large number of procedures to mitigate security concerns. These range from using individually serialized, numbered bar code seals that go on the touch screens and the AccuVote optical scan units. Those are then inputed into an access tracking system which allows us to track chain of custody. If that was changed, as Mr. Ronco said, in the sleepover event, there's no way that you could not find that out before the election happened or you would find it out election morning.

We also, you know, have solid procedures in place for securing our windows operating system, which is what the GEMS server runs on, anti-virus, as well as physical access to the server room where the GEMS server is held and the voting equipment in the warehouse. It has cameras on it, secured and audible access of the warehouse as well.

Any computer system, elections-related or not, without proper updates, patches, and procedures, will not be secure. And election equipment security requires a multi-layered approach and will always require a mixture of software, hardware and written procedures to ensure secure and accurate voting.

Thank you.

MODERATOR PÉREZ: Thank you.

Now I assume we have Lisa Thomas.

No?

MR. McCAULEY: I'll close.

Okay. Very good.

So we'll skip Lisa Thomas.

MS. THOMAS: I'm ceding my time to Jim McCauley.

(Laughter.)

MODERATOR PÉREZ: He's already achieved his maximum session. But thank you.

MR. McCAULEY: Jim McCauley, County Clerk/Recorder/Registered Voters for Placer County.

I've been in the election business for 33 years. I'm probably one of the last dinosaurs walking around. I can remember when we actually counted ballots by hand. And I can remember the criticisms we took in counting ballots by hand. And I can remember in L.A. County where you'd have one group that would run the election during the day and you'd have a second team that would come in at night and count the ballots. I can remember where I was as high as 38 percent of the precincts return when we had -- the county was incorrect, that we'd have to go back and audit.

I can remember the criticisms that we heard in this state from the paper ballot elections. And so we moved to the punch card. I can remember the criticisms of the punch card voting. So we moved to automated systems. Now the touch screens are stealing elections.

The election business is not simple. I've devoted my entire life to conducting fair and open elections.

In Placer County -- you know, what I wanted to show you today were examples of procedures that could be used to protect the environment of the election and the holiness of election day. And I'm sorry if I've taken up too much time in doing that. But I wanted to show you more, but I'm skipping over some of it.

But what it gets down to is that I don't believe the state has taken enough time to come -- nobody's ever come to Placer County and looked at my procedures. No one's ever come to Placer County to see all of our protection that we have in place. If you're going to make a decision by Friday, you need to make that decision based upon all the information that you can obtain. And I don't believe you're going to be able to get that information by Friday.

Now, you've had months in advance -- and please don't take this as criticism. It's just real as I see it. You had months to spend time in reaching out to the counties. Yes, we did get a survey. But that survey didn't even begin to touch what all the questions that needed to be asked about the system.

Should you trust me yet? No, I'm an insider. I need to earn your trust. You need to come in and take a look at how we operate, so you can walk away and say, "Yeah, they're doing a damn good job there."

That's why I set up the Advisory Council Committee in Placer County made up of citizens that had questions about the process, so they could become involved, so they could understand how the system works. So when they walked away, they said, yeah, they're doing the best they can to make it work.

Now, let's take a look at what happens at the polling places on election day. You know, we hear about the sleepovers. Now, you saw the bag. Now, if any of those seals are broken, the election board is instructed to immediately call our office. And we will take out a brand new machine and they will not use that machine to start the process. That's the beauty of optical scan voting, because voting continues even if the equipment breaks down for a few minutes.

They sign an oath prior to the election that they've examined the seals, that the seals are not broken. That's another layer of security that we try to put in place.

And I can speak all day long about procedures. And unless -- until the state takes the time to come to us to find out about these procedures, then I'm afraid that come Friday that you're not going to be able to make the best decision possible. and I know that time is a factor. I applaud the Secretary of State. It was a very noble idea to go ahead and investigate these systems. I've never been a fan -- and I'm not -- and please don't take anything I'm saying as criticixms of another county.

I've never been a fan of touch screen voting. Not because it doesn't work, not because it doesn't count properly. There were several factors that entered into my mind why I didn't want to go county-wide with a touch screen system. Number one, it's very expensive. I'm in one of the fastest growing counties in California. My voting population's going to double over the next 14 years. Model A, ten years -- years from now is going to be a better model. It was ridiculous. But I wanted my disabled voters to be able to vote. And I wanted to make the needs and the requirements of the Help America Voting Act for the disabled voter. So I had focus groups. I brought the disabled voters into my office and said, "Hey, what system is the best for you?"

And the system of choice. We've heard out there, the AutoMARK that has the paper trail. I found that system in Milwaukee. And I had them come out to California because I thought that system had a lot of merit. But investigating that system I also found out that system had a lot of problems. And it was the worst rated system from my disabled voter community when they looked at that system. They chose the touch screen system.

So, you know, we can't forget about those voters. And I really believe -- and I read the report as well as I could that came out in the amount of time we had to read. I believe that there are answers to a lot of these questions that have come out over this report. And I hope and pray you allow -- and come to the election community and allow us to help you with those answers.

Thank you for your time.

MODERATOR PÉREZ: Thank you very much.

Now we have Joan Lee, followed by Judy Bertelsen and Neal Kelley.

Joan's gone?

Okay. Judy Bertelsen.

Well, then we'll do -- is Neal Kelley in the room?

I don't see Neal.

There we go.

I'm going to list off the names of the next few speakers as Judy makes her way down.

Neal Kelley, if somebody could get him from out of the room; Michelle Gabriel; Sharon Graham; and then Diana Madoshi.

MS. BERTELSEN: I'm Judy Bertelsen. I'm a registered voter in Alameda County. And I want to thank the Secretary of State for conducting a from top-to-bottom review.

I also want to thank her for establishing a post-election audit standards working group and for appointing to that group not only a superb chair, Dr. David Jefferson, but a statistician and an auditor, as well as the other good members.

Because a review of computer systems cannot fully assure the security of any system, serious and well designed audits must be done of all election results. Our election audits should be as good as those used by banks and casinos.

The audit working group has made a major breakthrough, recommending a risk-based approach involving, in quotes, "the adjustible sample model where the size and the initial random sample depends on a number of factors including apparent margin of victory, the number of precincts, the number of ballots cast in each precinct, and a desired confidence level, for example, 99 percent, that the winner of the election has been called correctly."

This is a big step in the right direction. We will need leadership and guidance from the Secretary of State's Office about this, how to implement it. And we will need full cooperation from each of the counties, both registrars of voters and the county auditors.

The audits of elections should be conducted separate from the registrars of voters. It makes no sense to have the registrars of voters audit their own activity. It's a violation of basic principles of auditing.

We need to develop serious and professional standards for our audit procedures. It seems plausible that the county auditor might be the agent for the election audit. Certainly it's not appropriate that registrars of voters audit their own performance.

The risk-based approach can be applied by having the size of sample needed for each race determined by an auditor at the state level and informing the counties of the size of sample tests that would need to be randomly drawn and hand counted for each race.

Both the McCarthy Stanislevic paper entitled

"Percentage based versus SAFE Vote Tabulation Auditing, a Graphic Comparison," which is available at the Verified Voting Foundation website, which has been submitted for publication in an American Statistics Association journal; and the New Jersey bill, which was coauthored by Stanislevic, can serve to guide urgently needed plans for serious audits following the model recommended by the working group.

I thank from the bottom of my heart the audit working group as well as the top-to-bottom review teams for their excellent work under a very tight time pressure.

MODERATOR PÉREZ: Thank you very much.

Neal Kelley, Followed by Michelle Gabriel and Sharon Graham.

MR. KELLEY: Good afternoon. I'm Neal Kelley, Registrar of Voters for Orange County.

I want to begin by stating that the County of Orange fully supports a systematic review of our voting system. We use Hart Intercivic in Orange County.

It is an election official's duty to ensure that the votes that the system is tabulating has not been tampered with and is recording accurately. And I applaud the Secretary for her efforts in this regard.

In 2006, we purchased and installed the voter-verified paper audit trail system in each of our

9,000 voting units. As you know, this allows the voter to verify on paper what they voted for electronically and establishes a hard copy to verify that vote. Those printouts are used in the manual tally to further ensure the tally was accurate.

Now, I suppose it's just my luck, but in Orange County we have had some of the closest races in California in the last three years. Two California Senate races, one which was 13 votes apart on election night; and a Board of Supervisors race just a few months ago that was three votes apart.

I suppose I could say I've been dissected in Orange County. And in fact we really have gone into a hand count scenario. We went into an election trial that looked at all of our procedures, all of our systems as well as the count on the paper ballots and found it to be a hundred percent accurate.

This report brings to light, albeit extremely important, that extensive security policies and procedures are extremely important. Obviously the specifics of our plan in Orange County cannot be discussed here. But what I would like the public to know is that it addresses areas such as hacking, personnel, vote tabulation, tampering, discrepancies, ballot creation tampering, building security, and change of custody.

I want to use just a quick second to tell you a personal anecdotal story. I'm a private pilot. And flying near Ontario International Airport is very stressful, there's a lot of traffic. And flying along parallel to the runway one day I asked to deviate in front of the approach path in fog, about a mile visibility. And I was cleared by the controller. And they told me that a 737 was on final about six miles out. So I'm chugging along at the end of the runway there. And they call out five miles. Then they call out four miles. And I'm looking back and the pilot's looking for me. And as I passed through that approach vector I looked back, and the whine of the engines and the lights come through the fog, and we both acknowledge that we saw each other.

That is operating on 1950s technology that I have to rely on, policies and procedures, security and trusted personel, to ensure the safety of my life and those passengers on that airplane.

My point with all of this is that a review is extremely important. And I think it brings to light policies and procedures that may have to be mitigated or addressed. And it also brings to light the fact that many of us are doing all those things.

Thank you for your time.

MODERATOR PÉREZ: Thank you.

Michelle Gabriel.

MS. GABRIEL: My names is Michelle Gabriel. I'm a concerned citizen of Oakland, California, in Alameda County. And I didn't come with prepared remarks because I wanted to hear what was said and respond to them.

We've heard over and over and over again from many county elections officials about mitigation and how that wasn't looked for in the report. Let me just give you some quick personal examples of what I've seen with the mitigations. We've heard numerous times about tamper proof seals, and that poll workers are trained to look at the tamper-proof seals. And if they've been tampered with, that machine, something will happen.

First, I would like to say that this was also stated in the Alameda County Board of Supervisors by our ROV, Dave MacDonald. At that same Board of Supervisors meeting two people then got up and said that they had been in training and had not been told to check the seals. One of those was Dr. David Wagner, who we've heard earlier, a lot of kudos about who was doing the source code review.

So that was a great mitigation if it could have happened -- if it really happened consistently so it was implemented.

Then we have another one here where -- let's see, about the VVPATs. And the gentleman from Sequoia stated that he -- that how -- of course people look at VVPATs.

Well, let's see, what studies have actually been done? Recently Rice University's study came out where problems were properly introduced but people didn't catch them. Came out then during the audience, acting like -- to Stockton after an election.

And ask poll workers, you know, "What about those VVPATs?" And there's a poll worker on tape on a PBS show saying, "Oh, I told the voters don't look at that. That's for the people downtown."

That's on national news, okay? That goes around the world, believe me. These mitigations don't make me feel secure.

And then let's talk about the -- service attacks, okay? So we're going to have these mitigations. "Oh, my God, somebody's touched the tamper-proof seal." Now, what's going to happen? Are you going to take that machine out and service? Are you going to count those votes or not? That's the point. Are you going to count those votes?

So let's say somebody goes into one specific partisan area and quietly removes a seal, which anybody can do. Does that negate all those people's votes?

So when you look at these mitigations, I want you to think about also denial service attack. Not just securing, not just changing the vote but just totally annihilating the votes.

Now, I'd also like to make another comment. Mr. Steven Weir said that this study was a public policy blunder because no malicious source code was found and it was a missed opportunity. Well, gee, let me see, was the source code -- was a source code just taken out of a random machine? No, it was the source code supplied by the suppliers. That hasn't seen actual use.

Has anybody actually looked at any of that? My understanding was also that the ES&S source code that was taken out of escrow did not meet the actual what's being in use. Did anybody look at that for any of the other vendors?

You know what, I -- so I really have a hard time with the fact that, oh, the county elections officials really want to work with the Secretary of State about this, yet keep saying what a policy blunder this is and how they weren't allowed to participate in it. Maybe there are real reasons for that.

Thank you.

MODERATOR PÉREZ: Thank you.

Sharon Graham, followed by Diana Madoshi and Kim Alexander

MS. GRAHAM: My name is Sharon Graham. I'm not from Placer County.

(Laughter.)

MS. GRAHAM: I'm from Sacramento.

One technology that hasn't been discussed here today, which costs only one-tenth of those technologies which have been discussed, and boasts a 200-year success record -- not perfect, but successful -- adequate at least for 200 years -- is hand-counted paper ballots.

Dr. Judy Alter gave you some petitions that have been signed. This was a very low tech grass-roots effort by a very few number of people, both signatures and collectors. I was one of the collectors and one of the signatories. And I'd just like to -- there were about 1900 of us involved in this -- just give you a flavor of what is in that petition.

It starts off, "We, the undersigned, citizens of the State of California, have the right to expect that our votes be counted, accurately counted in public without fraud or secret software."

"We do not want Diebold, ES&S, Sequoia, Hart Intercivic, or any voting machines. We demand that the voting process be controlled publicly, not privately. We demand that local, state, and federal government officials control, inspect and understand these processes.

"Hand-counting paper ballots at precincts is the vote counting method least susceptible to fraud. Therefore, we request that you write legislation requiring the use of hand-counted paper ballots at the precinct level, as do most of the world's democracies, including Canada and Germany."

Thank you.

MODERATOR PÉREZ: Thank you.

Diana Madoshi, followed by Kim Alexander and John Tuteur.

MS. MADOSHI: Thank you for the opportunity to come here and to give my remarks as a concerned citizen.

I have to say I've come -- I've been at some of these proceedings before. And one of the things that has -- one of the things that stands out, every time the vendors come and we're talking about software versions, it's always been a new version that no one has seen. So as a skeptic member of the public, that sort of makes me even less concerned about their interest as far as -- my interest as far as the elections. To me it comes down to money.

I've heard a lot of talk about this up-and-down system, the review. I, for one, am glad to hear it, that we -- at least the initial step has been done. I happen to live in a county, Placer County, where I have a lot of confidence in our voters' registrar you heard, Jim

McCauley. But as much as I respect Jim, I also am involved with other voters throughout the state, and we don't have the confidence in the vote. We don't have the confidence as far as our voting being counted, especially by machines.

We have been told that there was no problem in 2002, people of color. We've been told that there have been no voting problems with Ohio and all sorts of other places. Yet, it has become documented that that is so.

So the public really -- and really is concerned about the sanctity of our vote. So I'm asking you, the Panel, to really take serious these concerns that have been raised by this red team and also to really implement a lot of safety features.

I have concerns about machines that are kept, sleepovers. Jim McCauley had his -- we had talked about that and he assured me that there is -- at least in Placer county. But a lot of other counties, from what I've heard, they don't have a lot of those safeguards. We need standardization up and down California, not just in Placer county -- what is being done in Placer County to protect the vote. It should be done the same in Orange County, Yolo County, any other county. Those things should be standardized.

And as far as -- and the other thing, registrars of voters, it's not an adversary thing to have to get this reviewed. I'm sorry if -- I get the feeling that some people thought they were being -- there time was being stepped on. And I know my time is up, but I just want to say this: We're all in this together. We are the consumer. I've heard the vendors call his customers. We are his customers. The voters of California are the customers and we're the ones that must be satisfied.

Thank you.

MODERATOR PÉREZ: Thank you.

Kim Alexander, followed by John Tuteur and Jennifer Kidder.

MS. ALEXANDER: Good afternoon. I'm Kim Alexander with the California Voter Foundation. We're online at calvoter dot org. Thank you to the Secretary of State and staff for assembling an all-star lineup of computer and security experts to study our voting systems. This review benefits not only California voters but voters nationwide. And it's occurring at a time where other states, particularly Florida, Ohio, and New Jersey, are undertaking similar exercises to study their state voting systems.

I've looked at the reports that have been released so far and am extremely concerned about a couple of findings. One of them is the finding that the Diebold

TSx touch screen machine has a remotely accessible Windows account that can be accessed without a password. That's a serious security risk that we need careful attention for.

Another one that was identified is in the Sequoia system, the boot loader and the firmware for the boot loader can be overridden, which is a problem that was identified in the Diebold system in a previous election. And so we now see a similar problem with Sequoia. So those are some serious risks that need some attention.

And security cannot be dependent on procedures. There are some procedures that have been stated that include delivering machines to poll workers' homes or to polling places several days before an election. And procedures at the local level may vary widely. It's difficult to monitor compliance in all 58 counties and all 25 precincts and by all 100,000 plus poll workers.

As the registrar from Los Angeles stated, paper ballot boxes have been stuffed in the past, presumably under the watchful eyes of poll workers. So we know that poll workers can't keep an eye on everything that's going on in the polling place.

The Secretary of State will need to consider both short-term and long-term options to address the findings of the report. For the long-term, we need to consider reengineering our entire voting system from the ground up, one that builds security in on the ground floor of the system. In the short-term, we may be able to mitigate risks through better security policies and better post-election auditing.

And as was mentioned, I just recently have been serving on a working group and our report was just published Friday. And we made a number of recommendations to the Secretary of State for strengthening California's manual count process. So I encourage you all to go online and read that report.

And I want to again thank the Secretary of State for taking the time to do this review, and to all of you for the hard work that's gone into it. And I look forward to seeing the remaining documents that have yet to be published.

Thank you.

MODERATOR PÉREZ: Thank you.

John Tuteur, followed by Jennifer Kidder and Richard Tamm.

MR. TUTEUR: Mr. Moderator, members of the Panel. I'm John Tuteur, the Napa County Assessor/Recorder/County Clerk and Registrar of Voters.

Napa County has been using Sequoia voting system's federal and state certified Edge 1 touch screen equipment since March 2002 on a pilot project basis and since March 2004 on a full fledge basis.

We have also been using Sequoia voting system's federal and state certified Optech optical scan paper ballot and 400C central count tabulation system since March 2003.

Over 105,000 electronic ballots have been cast on our touch screen machines and a slightly smaller number of optical scan ballots.

Our county invested in touch screen technology only after 1700 voters, ranging in age from 18 to 97, unanimously found the system accessible, secure, and voter friendly during our pilot project.

There's never been any question about the accuracy or security of the touch screen results for the five statewide elections that we have conducted since the pilot project concluded.

Our county invests -- excuse me. We have used Sequoia's optical scan paper ballots in seven major elections beginning in March 2003. We had a contested supervisorial election in March 2004 involving optical scan ballots that went to Napa Superior Court. The Court found our conduct in the election was correct and upheld the final results.

California's post-election procedures such as the one percent manual tally have proven that the final results of electronic and optical scan voting systems are accurate and able to withstand judicial scrutiny.

In November 2006, a losing candidate in a municipal election paid for a recount. We hand-tallied over 2,000 paper trail ballots and over 1300 optical scan ballots. The hand-tally did not vary by a single vote from the electronic results that produced the official canvass.

Attached to this statement are six pages of statutory, Secretary of State, or vendor-suggested procedures we have in place to ensure accurate and secure elections. And I'll just hold those up so you can see. I've submitted them already to Debbie O'Donahue of the Secretary of State's staff. So I have them here, but you've already got them.

The top-to-bottom review has no relevance to the real-world conduct of elections within the framework I have just discussed and has wasted almost $1 million of scarce federal funds. This top-to-bottom review deserves the same admonition that I gave to former Secretary Kevin Shelley after his decertification fiasco.

Secretary Bowen, you should know better than to erode the public's confidence in California's fair and accurate elections process for crass political purposes. Shame on you.

MODERATOR PÉREZ: Now we have Jennifer Kidder, followed by Richard Tamm and Jim Soper.

And before Jennifer Kidder starts, we received one written comment for somebody who chose not to stay. So we're accepting a written comment from Kathleen Persons.

Go ahead. You've got six minutes.

MS. KIDDER: Yes, thank you.

I'm here to speak in enthusiastic support of Debra Bowen in taking bold, strong action to prove what we have been impressing upon our local officials and politicians for a good four years, and many of us for more, to little or no avail.

I'm here, first of all, to speak as a disabled person. I need assistance. I need accommodations different from others in order to give me an equal opportunity at success; an equal opportunity to have my voice heard, for instance, in Berkeley when I got my Physics and English degree. Not sitting in the same classroom with my classmates for the same amount of time. But for a true account of my knowledge and effort to be expressed and heard, by my professors in that case, equally with my classmates, I need an unequal experience of the measure of it.

The exercise of voting is for the purpose to get our voices heard, to control and affect our own government. It is not for the experience of the exercise of voting itself. The purpose of the secret ballot is to combat intimidation or coercion by others to manipulate and change and, thereby, steal that vote. If that vote can be changed or erased after that private experience of voting, the whole exercise of voting is useless. The right to vote is stolen after the active voting if the count or record of that volt is stolen, out of sight or out of other verifying senses of the voter.

I just want to remind all our government representatives and official that the purpose of any equal opportunity legislation is to get marginalized voices heard to affect our world and, most importantly, our government, to equally choose who represents us and runs and controls our government. I do not trust any secret software corporation, privately owned, who designed and -- designed and controlled computer to accurately or honestly express the voice the true intention of disabled voters, including myself.

And if I have a disability that in certain circumstances requires assistance, I want the assistance to come from a human being I can communicate with and do trust more than a privately-owned corporation and their programmers, whom I do not know, but who I know do not have my interests but, on the contrary, profit as their motive.

For that reason, it is why I am also here more fundamentally as a hand counter paper ballot advocate, for only directly observable by sensory perception vote recording and vote counting can truly express democracy where all can vote and witness without breaking of the chain of custody the counting of that vote with our own senses. Democracy is not based on faith and secrecy but accountability and transparency.

The most important accessibility is accessibility to the process by which we choose our representatives and control our government.

And I also want to say in that respect that public ownership and control over that system devised by our founding fathers by which we the people control the public sector, our government, must be in no way under the ownership or control of the private sector. Private corporations, by law, corporate persons -- law, which also must be abolished, have profits, not the public good, as their primary motive.

So I don't know where I am on my time. But I just want to say that publicly owned and operated and entirely observable voting systems are the only things that we should trust with a democracy. That's the entire idea of democracy.

Thank you.

MODERATOR PÉREZ: Thank you.

We now have Richard Tamm, followed by Jim Soper and John Longoria.

MR. TAMM: Good afternoon. Thank you, thank you, thank you, thank you so much, Debra Bowen and all of you who have been working so hard on this project. My name is Richard Tamm. I live in Berkeley. I'm not from Placer County.

And I've been a programmer for over 30 years. And I know from that experience that, as far as I'm concerned, anything -- any kind of code could be hidden in these machines and it would be practically impossible to find it.

A number of people have said no malicious code was found. Well, I thought the very Panel said that no malicious code was looked for because it is such a massive job, and even then it may still not be found. It could possibly hidden even in what we call object code, which is just a series of 1's and 0's, which would be impossible to interpret.

I just want to say something about exit polls. The state of the art of exit polls have advanced to such an extreme -- such a point where they are extremely accurate. Some European countries that have hand-counted paper ballots use exit polls to declare the winner before the ballots are completely counted, because the exit polls have been found -- over time they've perfected -- they have been found to be that accurate.

I've also heard a number of people say there have been no smoking guns for stolen elections using these machines.

Well, there are smoking guns. It's the exit polls of the 2004 election and the 2006 election. 2004 election, among other things, there was a book written, "Was the 2004 Presidential Election stolen?" If you researched it at all you know that the exit polls in all the swing states in 2004 showed Carey leading by a few percentage points. Late in the evening they all switched -- the actual count all switched over to Bush outside the bell curve of possibility of these exit polls.

To me, that is so suspicious, and it points to massive fraud using these machines.

In 2006, the day after the election, the Washington Post reported that all the major news agencies late in the day stopped using exit polls because they found they were skewed 6 to 8 percent toward the Democrats, again indicating I think massive fraud using these machines.

I trust Diebold ATM machines because I can check my bank account and I know bank auditors are extremely rigorous in auditing the banks.

I don't trust the voting machines because I can't check that my vote was recorded as I made it or tabulated as I made it. And I don't think there's ever been an audit of an election nearly as rigorous as a bank audit.

I applaud you in doing the red team attack, all that work testing, because I am most concerned about secret malicious internal code, not the hacking. And I think it was very appropriate for that.

And thank you very much. And I again applaud you all and Debra Bowen.

Thank you.

MODERATOR PÉREZ: Thank you.

We now have Jim Soper, followed by John Longoria and Candace Grubbs.

MR. SOPER: Good afternoon. Ten minutes?

MODERATOR PÉREZ: You have nine minutes.

MR. SOPER: Nine minutes. Okay.

My name's Jim Soper. I'm a senior software consultant and programmer for over 20 years. And I've been involved in election integrity issues for almost two and a half years now.

One American, one vote, counted as cast. That's the motto at the top of my website countedascast dot com. And that's what we're here for, all of us. And I recognize that we're all here to fix the elections and -- not fix them bad but --

(Laughter.)

MR. SOPER: -- make them good.

None of us are here to rig elections. Let's be clear on that.

Let's also be clear that the California State law says that these elections, and the machines must be safe from fraud and manipulation. Indeed, I think they should be safer from fraud and manipulation than slot machines are in Nevada. And we're working in that direction, but the slot machines still win on their security.

I want to address a couple things more technical for the moment. One is the issue of the red team had access to source code. Well, this is not a game. This was an exercise, a professional exercise to try to assess as much as they had in the time they had to find out what we really are dealing with. And if you want to play games, you can play games of what's the reality. But that wasn't the point of this. This was to get as full an assessment as we could, and I think they did. They did a very good job in the time they had.

Also with the idea that the red team had access to source code, they say clearly at the end of the Sequoia paper they didn't need it. You could do everything you did without the source code.

In the case of Diebold, we had the source code. It's out on the Internet, surprise, surprise. And encryption keys that have been there for, well, now, ten years are still there. So this is just -- we got the source code there.

Three, to the best of my understanding -- and I would stand corrected -- they also did exploits with Windows and the central database. It's both on the Sequoia and Diebold machines. The central database is a Microsoft product. They had no access to the source code for Windows or the Microsoft databases, and they still did things. And they did things through the central data bases, which is what scares me the most, because I fear -- if you read about the security problems, the insider attack is more dangerous and more likely to happen than putting viruses in from the precincts. So they didn't need source code for that either.

And, finally, I don't know of a screwdriver or a minibar key that has source code. You don't need it to open up the machines and they still successfully open up the machines, still keeping security tapes in place, and things like this.

Next point. The gentleman from Hart said several times that they started on their work in 2003 and they had no guidance from the election community about what to do. I'm sorry, this is disingenuous. You had the 2002 voluntary voting system guidelines. They existed. Please don't say you had no guidance. Now, I know the federal guidelines are not very good and they still need to be improved a lot. But don't stand up here and repeat a message that you had no guidance when you had some.

Then they said, "Well, gee, we wish we had time to respond" -- this is Hart -- "respond to the report. And, gee, had there been time, I agree, that would have been a good thing. But we have to get ready for a February election." And I note that it was in the report that Hart did not help the team with the firmware update program. That delayed the team. So Hart was not interested in time. They were interested in stonewalling.

Parallel testing, really quickly. I haven't read -- I read a report of parallel testing from a few years ago. They selected the machines to be parallel tested at least days before the election. They knew which machines were going to be parallel tested. So that's not a random selection of machines. That's not a fair test of parallel testing because somebody can go in and tell a machine that you're going to be tested so behave properly.

If they do parallel testing, they have to do it right, random selection of the machines on election day.

Mr. Weir correctly, and grabbled, asked the question, "Is there malicious code in our software?" Well, we don't know what's in the machines. I stood up here -- or I contacted previous Secretary of State and asked, "What ae the procedures to confirm that the code that is in escrow is the code in the machines?" The response I got was 'We're working on it."

And I asked Dr. David Wagner later on, who was involved with this, "Am I crazy or we don't know what's in the machines?" And he said -- well, you're right. So we don't know what's in the machines. I think we are moving towards getting that done. I know Mr. Weir did some things at Kennesaw State, I believe, that was moving in the right direction. But we need to have that procedure done all the way through. And the firmware, I noted in one of the reports, I can't remember which machine, we don't -- there's no way to know what firmware is in the machine. So that's a problem.

We have talked about this study -- the red team study was not reality based. Well, let's take a look at reality here for a second. We have a Monterey registrar that's sitting in jail because he's dishonest. We have audit data that's been fudged in Alameda County. We have a one percent audit that's not enough to check real stealing of votes in precincts. We had over 400 Sequoia memory cards lost in Chicago last year, 75 in Cleveland last year. I know of one that was sort of locked up, but you can't be sure, in a county, and I'm not going to say which county because I don't want to embarrass people. But -- and I don't think anything happened there. But they can't keep control of all of these thousands and thousands of cards. You really have to be very careful with that.

We have sleepovers. We have at least all night if not days or weeks to play with the machine, play with the machines, maybe get ahold of the serial number of the tape and go to the manufacturer of the security tape and get it copied with the exact same serial number. Take one tape off, put the same one on.

There are machines that could be opened with minibar keys and screwdrivers.

We have a situation where we know Diebold lied to the California Secretary of State in the State of California. So we can't trust them. And we know that it only takes 90 seconds to handpack the GEMS database. And Howard Dean could do it. This is the reality.

We also know now some people have been saying we want to have a real test, a real situation. Well, where were you last year in Alameda County when we stood up and the Board of Supervisors voted for a security test, also known as a hack test or a red team test? And that was suppressed by the registrar. They were ready to -- the team we had assembled was ready to do it for free. And the county backed down. And I understand there's a similar situation that happened in a Sequoia county, where they -- there was a challenge to do the test and they were ready and the county backed down.

Where were you? Now you don't like it. But here we've got to do the best we can. And we've had a very good professional job.

I want to thank Debra Bowen very much for doing exactly what she was voted -- for doing exactly what she said that she was going to do. She was voted in by the people of California. This is what the people of California wanted. And I say, "Bravo, Debra Bowen."

Thank you very much.

(Applause.)

MODERATOR PÉREZ: Again, we're not going to have applause, booing, any other demonstrations of support or opposition. They're going to take us away from our comments.

Our next speaker is John Longoria.

When Mr. Longoria is done speaking, we're going to take a 15-minute break. When we come back from the break, our next three speakers will be Candace Grubbs --

MS. GRUBBS: I will pass.

MODERATOR PÉREZ: I'm sorry?

MS. GRUBBS: I will pass.

MODERATOR PÉREZ: Okay. Brandon Tartaglia and -- I can't make out the first name, but the last name is Reese. Maybe Preston Reese.

Okay. Very good.

So go ahead, Mr. Longoria.

MR. LONGORIA: Thank you, moderator Perez and panelists and Secretary Bowen. My name's John Longoria. I'm an advocate with Disability Rights Legal Center in Los Angeles. It's a nonprofit civil rights law firm whose mission is to promote and protect the rights of persons with disabilities.

While we're in the process of conducting a more thorough review of the results of the top-to-bottom review, and do plan on submitting written comments, we nevertheless thought it was important to be here today and express our primary concern in terms of the accessibility review segment of the report.

Well, we too believe and support the Secretary's efforts to ensure that California voters can cast their ballots on voting systems that are both secure, accurate, reliable, and accessible. Our paramount concern again is the vote disenfranchisement that will and possibly ensue should any of these voting systems that are presently certified become decertified.

Without question, much still needs to be done to improve and ensure voting systems are physically accessible and usable for persons with disabilities -- of all disabilities in California.

But, as one previous speaker adequately put it, let's not throw out the baby with the bath water.

We strived and voter participation has increased. There's greater accessibility. We don't need to turn back the time and deny a fundamental right to people with disabilities who want to participate in our democracy.

That being said, I think the review provides an outline in terms of what needs to be addressed in some instances, provides some recommendations. And clearly there are, you know, what can only be called the oversights in the worst case where voting systems are deficient in the most basic levels, as one of the previous speakers pointed out, the clearance in terms of, you know, a wheelchair user or a scooter user being able to access a voting equipment device is not possible in some of those systems.

And those were, again, systems that were certified by the previous administration and Secretary of State's Office.

So there are things that, again, with the help of the elected officials, with the help of the vendors, with everyone's assistance can be easily and quickly cured in terms of some of the more obvious deficiencies.

So we look forward to working with the Secretary of State's Office, other advocates, the vendors and the elected officials to improve the systems.

And, again, we want to stress that we don't want to disenfranchise voters and take this to the extreme and have a measured response, a reasonable and practical response to this report.

Thank you.

MODERATOR PÉREZ: Thank you.

With that, we're going to take a 15-minute break.

I show it being 3:42. So we'll come back just a few minutes before 4 o'clock and reconvene for the duration of the afternoon.

And I only anticipate about another hour's worth of public comment. So we should be ending right about 5 p.m. Thank you.

(Thereupon the Voting Modernization Board
meeting recessed at 3:42 p.m.)

MODERATOR PÉREZ: Is Brandon Tartaglia in the room? Great. Preston Reese, Brandon. We'll start with Brandon Tartaglia in just a second, and then Preston Reese, followed by Jerry Berkman.

So if those who are in the room would take their seats, we'll get started.

Go ahead, Mr. Tartaglia.

MR. TARTAGLIA: Hello. My name is Brandon Tartaglia. And I'm with Protection and Advocacy, an organization mandated to advance the human and legal rights of people with disabilities. Thank you for the opportunity to comment.

We have reviewed the Accessibility Review Report for California that concludes the Hart, Sequoia, and Diebold electronic voting systems to be non-compliant with the accessibility requirements of HAVA and the 2005 voluntary voting system guidelines.

We would like to express concern that the report's findings may lead to a decision to de-certify all or some of these voting systems, thereby precluding countless Californians with disabilities from exercising the right to an accessible, private, and independent vote. The Accessibility Report identifies deficiencies with the reviewed systems and also recommends short-term and long-term mitigation strategies to address the deficiencies.

We agree that a short-term strategy can mitigate a number of the identified problems. The report does not, however, also recommend decertification of any or all of the systems as either a short- or long-term strategy. We agree with this finding as well. Decertification without an identified and readily accessible replacement system will result in a disenfranchising of the disabled community at a critical time in our nation's history in violation of federal and State law.

We support you in adopting a short-term remedial mitigation measure for the near-term 2008 elections as an alternative to de-certification. We urge you to advise county election officials as well as the Hart, Sequoia, and Diebold vendors to implement the measures identified in the report. For the long term, we urge you to actively seek out, review, and certify new technologies and voting systems that refine and enhance the promise of an accessible, private, and independent vote for Californians with disabilities.

We would like to work in collaboration with the Secretary of State and other disability rights advocates to help ensure that the voting needs of people with disabilities are fully understood and addressed. Thank you.

MODERATOR PÉREZ: Thank you very much.

Next we have Preston Reese, followed by Jerry Berkman and Kari Verjil.

MR. REESE: Good afternoon. My name is Preston Reese, and I want to say thank you so much. I actually think this is the most important hearing that's been held in California for ten years. I think this hearing is the reason that Debra Bowen won the Office of Secretary of State. And I want to give my thanks to Secretary of State Bowen and to each of you.

The vote is precious to everyone. And I have the utmost respect for those who are registrars. But I'm also a very experienced computer user, as many of you are. For 15 years, I've used Microsoft Windows very happily. I think they make wonderful products.

And one of the vendors complained one of the tests was conducted on an old version of Windows 3.1. And he instead recommended Windows 2000 or XP. Windows 2000 was a very stable system. But like all software, there were ways to get into it and create problems with it. And according to a lot of the people in the industry, there's essentially an army of teenage boys -- not to stereotype -- but there's an army of teenage boys and others who are always working toward this. And that's why Microsoft continuously was releasing patches and fixes for these various problems that would come up.

When enough problems accumulated, they released them on a CD called Service Pack 1 and then Service Pack 2, Service Pack 3, Service Pack 4. So you see where I'm going with this. It doesn't really matter what system, what computer, what operating system or even what firmware you're using, you are looking at a system that is going to be vulnerable.

Now, if the nation's most popular operating system is vulnerable to this army of teenage boys, you can only imagine what the kinds of motivation could be involved in people with a lot of money and a lot of power to do something with the software or firmware or any other aspect of the computerized elections.

So I do support the idea of returning to paper ballots with a continuous trail. And I want to thank each of you very much and the scientists who conducted this excellent work that exposed some of these flaws. Thank you.

MODERATOR PÉREZ: Thank you.

Jerry Berkman, followed by Kari Verjil and Barbara Dunmore.

Mr. Berkman, you are with RTF?

MR. BERKMAN: Yeah. Among others.

MODERATOR PÉREZ: I'm sorry?

MR. BERKMAN: Among other organizations.

I had two people cede.

MODERATOR PÉREZ: Yes.

MR. BERKMAN: Okay. I just gave the Panel some prepared testimony, but I'd rather for now I'm going to respond more to what people have said.

I'm Jerry Berkman, a retired program -- could you warn me when I have three minutes left also and then half, so I'll know to speed up if I'm slow.

Thanks for doing this top to bottom review. At the U.S. Senate hearing last week, on the HR 811 and S 1487, the Electronic Technology Association gave Senator Finestein a timetable. It says that major upgrades take 54 months.

Okay. So let's look at what this means. Our current systems are not fully accessible and not secure.

First, accessibility. The report says systems are not fully HAVA compliant. They don't worry about the California Elections Code, but we know they do not satisfy Election Code 19250(a) and 19251(a) and that the path is not accessible.

So do we want to wait 54 months? That means maybe we would have that by the elections -- the general election in 2012, but not the primary. In fact, one of the election officials at the hearing said we should wait for 2014, because that's a relatively quiet year and we can really get it right. That's crazy; right?

Professor Doug Jones, the University of Iowa, has a patent on an assistive device. Why not look into that? Or as Dan Kaiser said, why don't we have research into assisted devices or something, some way to do it faster?

There's the group -- the University of California has a center which investigates the interface between technology and society called citrus. I don't remember what it stands for. It's multi campus. It would be ideal to give them some money, especially to look into assistive devices. Similarly, do we need to wait until 2012 or 2014 until these things are secure?

In 1995, in Louisiana, the Republican loser went and inspected the DREs in the warehouse. That's twelve years ago. They wouldn't register votes for her, which is why she lost. And she tried to appeal and got nowhere. You can see that in Voter Gate or Hacking the Vote. Voter Gate is on the web. So twelve years ago. And they have video of her punching the buttons and her opponent's name coming up.

The Sequoia rep told us we need background checks on election workers. It's too expensive and difficult to do this for all the poll workers. I don't think any registrars really do that for all their poll workers, do they?

In their answer to the Alameda County RFP, one of the questions is, what background checks do you do on your employees? Sequoia said basically it's none of your business. They won't tell us whether they do background checks on their employees or what kind. What are they afraid of?

How many Sequoia employees have had access to the Sequoia source code in the last eight years? How many Diebold have had access to Diebold source code? If it's like ten, it's probably still secret. If it's a thousand, they probably have a lot of programmers moving in and out and getting other jobs. IT isn't that stable. The secret -- you can't guarantee this is still secret if they've had a thousand employees with access to the source code.

Anyone who's serious on security would not use Windows. Ask anybody who has a security background. They use Linux or FreeBSD or MAC O S, et cetera.

So what you're using there, is that a MAC or what?

PANEL MEMBER FINLEY: Windows XP?

MR. BERKMAN: I thought when he asked about the viruses.

I looked at the Riverside County SOVC, Statement of Vote Cast, on the web and the Governor's race. There were four precincts that had zero registered voters and one vote for Governor. How does that happen? No registered voters, but there's a vote for Governor.

Am I supposed to believe all these systems really work reliably and accurately, never any error when I see that published on the web? Seriously, I would have looked at other counties, but I don't think they're all published.

I think there ought to be a regulation that all of these SOVCs should be published on the web in a common separated values format or Excel or something rather than a PDF. I only looked at the Governor's race because it look 20 minutes to cut and paste that into my system so that I could look at it. It should be available for anybody that wants it.

Each county should do that, except may be the ones that only of a thousand voters or 2,000. I don't want to -- you know, L.A. has two million five -- millions of voters, and some have only a thousand voters. And you can't do the same thing everywhere.

We need transparency. Let's -- citizens are shut out. I was an Election Code 15004 representative last election, which means you're supposed to be able to observe any and all aspects of the election. But when I asked to see the logic and accuracy test close enough to see something, they called the sheriff. There were four sheriff deputies behind me. This was after I had an operation. So I'm standing there on two crutches with four sheriff deputies behind me to make sure I don't get out of -- make any trouble.

Can we see the logs? I'd like to see these event logs the logs they're talking about that tell us about all the errors. Because I doubt if all the registrars go through these with a fine tooth comb.

And policies and procedures should be put on the web also. There is big stakes. How much is a U.S. Senate seat worth? Right now, there's 49 Republicans, 49 Democrats, two independents. And what is it worth if you want to fix a Senate race? Probably, what? How much would they be willing to spend? A couple million dollars? They could hire some serious hackers to do that and some do some serious social engineering.

Also, for the registrars and the vendors who say they were shut out of the top-to-bottom review, the election activists also were shut out. We didn't really have any access to what was going on. I had some ideas, but all I could do was send them in after the public hearing.

I think basically that's fair that the Secretary of State should really decide what's best, rather than listen to everybody but not give anybody access.

Okay. And then from my prepared testimony. Opponents claim we need electronic voting systems to get fast, accurate results on election night. However, now that about 50 percent of the ballots are absentee, the final election night total includes as many absentee ballots as electronic ballots and definitive totals are not available for weeks.

They also say we need DREs for HAVA compliance. However, the vendors made only a half-hearted effort to make accessibility. We need to look at other solutions. And the thing that Doug Jones does on the web, he said it would cost $200 or less for an accessible device.

We need to de-certify the DREs. Mitigations are rarely effectively and consistently implemented. For February, allow one DRE per polling place for partial HAVA compliance. We know they don't fully comply.

And a couple things. People talk about theoretical and you get this false sense of security. Did you know that some car keys have RFIDs in them? So that only that car key is supposed to be able to start the car. RFID is -- I don't know what that is. Some techy thing. It turns out that the tow companies were having problems, and so the vendors -- the car companies put in codes which you can get. So that instead of using a key that matches the RFID thing, you can actually do a sequence on the brake and start the car. And the tow companies have access to this.

Similar -- and also Ed Felton at Princeton and his students figured out a way without touching the key but being within a couple feet to duplicate that.

So we all think these are safe, but they aren't. And the same thing with our home locks. It turns out there's something called a bump key you can get on the Internet that will open most of the homes without seeing the key. Okay. Thank you.

MODERATOR PÉREZ: Thank you, Mr. Berkman.

Next we have Kari Vergil, followed by Barbara Dunmore and Douglas Kinzle.

MS. VERGIL: Good afternoon. My name is Kari Vergil, Registrar of Voters for San Bernardino County. I have 15 years of elections experience. I worked my way up through the ranks and now am Registrar of Voters for San Bernardino County.

What I've learned over the past 15 years is that elections officials are dedicated and ethical individuals. Their staff work long, hard hours to ensure the integrity of the election process.

I support the comments made by our President Steven Weir today. And I'd just like to take a couple minutes of your time to talk about San Bernardino County.

San Bernardino County has over 700,000 registered voters and is the largest county in size in the nation. Our precinct voters have been casting ballots since 2004 using Sequoia's Edge II voting equipment. We have an inventory of 4,000 touch screen voting units and 5,000 voter verifiable paper audit trail units.

San Bernardino County was the first county in California to implement the paper audit trails. Feedback from our voters regarding touch screen voting units is positive, and they are confident with the system.

Our absentee voters cast their ballots using Sequoia's Optech paper ballot system. Again, our voters are confident and positive with the system.

Our county has been selected on two occasions to participate in the Secretary of State's parallel monitoring program. Most recently, our county was selected to participate in the program for the November 6th gubernatorial election. The results were successful for our county as well as all of the other counties selected.

All counties adhere to strict security procedures, and they are strictly enforced. Free access is not permitted to any voting system or components.

I'd like to give you just a couple examples of some of the procedures that we have in place in San Bernardino County.

We have chain of custody procedures that track the location of equipment from storage in the warehouse to programming and delivery to and from the polling places.

Our poll workers attend extensive training and are required to verify the equipment serial numbers and to ensure that no tampering occurs with our voting equipment.

Our touch screen VeriVote printer units, card activators are stored in a secured alarmed location.

Our election staff works diligently and are dedicated to the election process and have undergone background investigations.

I encourage the Secretary of State to work with Registrar of Voters. Our office is open to all, including the Secretary of State and her staff. You are encouraged to visits our office. Our goal is to continue to conduct successful elections. Thank you.

MODERATOR PÉREZ: Thank you.

The next three I have are Barbara Dunmore, Douglas Kinzle, and Wayne Beckham, all three from Riverside. Would you like to do this individually or would you like to --

MS. DUNMORE: We'd like to do individually, please.

Good afternoon. I'm Barbara Dunmore, Registrar of Voters for Riverside County. I'm here today to share with you information regarding Riverside County's experience with Sequoia Edge I voting units.

Riverside County has the longest history in the state with electronic voting, having been the first county in the nation to deploy the technology county-wide during the November 2000 Presidential general election.

Since its implementation, 39 successful elections have been conducted with Sequoia DREs without any errors or defects. Moreover, no known or documented attacks designed to manipulate the system has been reported in Riverside County or elsewhere.

In the past seven years, Riverside County was audited twice through the Secretary's parallel monitoring program, and our voting system performed with 100 percent accuracy. Post-election audits have verified that voters' selection were reported and tabulated accurately. And the voter requested recount has never changed the outcome of an election in our county.

Voters in Riverside have a choice, paper or electronic. Since 2000, Riverside County has conducted elections using two voting systems: Sequoia Edge voting units in the polling places, and DFM Mark-a-Vote paper ballots for absentee and paper requests at the polls.

While 40 percent of voters vote absentee in Riverside, less than one percent of polling place voters request paper ballots. Our voters know that they have a choice. And when they walk into a polling place, they expect to cast their ballot on a touch screen voting unit.

The majority of voters have expressed their trust and confidence in electronic voting through their actions at the poles. As responsible election officials, we have shown flexibility in responding to legislative changes aimed at enhancing voter confidence and improving security such as the addition of the voter verifiable paper audit trail.

It is ironic that election integrity advocates who so aggressively pursued this policy change now want to abandon it after millions of dollars have been spent on purchasing printers and their accuracy and added value proven. The environment in which the red teams conducted their attacks can only result in an erosion of confidence in the democratic process we all work so hard to protect.

The methodology lacked physical security measures and constraints on attackers and offered no evaluation of the feasibility of such attacks under real world conditions. Testers were given all the information the Secretary of State had, much more than election officials have access to, and were told essentially here's the combination to the safe. See if you can break into it.

I'd like to end by giving you a primer of the real world environment of election offices. Election offices include security cameras, isolated tally services, strict chain of custody, tamper evidence seals, bar code tracking, background checks, audit logs, restricted access, user authentications, leased privilege policies, check and balances, and much more.

Our mission as election officials is to assure the public's will is reflected in the results of the election. And I remain optimistic in her measured approach the Secretary will continue to allow Californians to choose the method they desire to cast their ballot, electronic or paper. Thank you.

MODERATOR PÉREZ: Thank you.

Doug Kinzle, followed by Wayne Beckham, followed by Dan Ashby.

MR. KINZLE: Good afternoon. There's three of us, but we all have three different flavors of this. So my testimony today will sound familiar I think.

Today's public hearing was called to give interested persons an opportunity to express their views regarding a top to bottom review of voting systems. So I will.

In the words of the Secretary of State, the review is designed to restore public confidence in the integrity of the electoral process and is designed to ensure that California voters are being asked to cast their ballots on machines that are secure, accurate, reliable, and accessible.

Since accuracy and reliability of these systems was not addressed in this review, one can only conclude that this exercise fell short of the stated goals. This review was only half of the pie performed on half of the systems in California. And the overall conclusion at this point cannot be made.

Furthermore, the systems were examined in laboratory conditions where vulnerability was found in some areas that are protected in the real world by means that they did not test. In this exercise, if this exercise was to simulate a hacker's assault on a real world voting system that could go undetected, that was not proven by the Red Team. They make no claim as to the feasibility of such an undetected attack that would successfully change an election result. They made the case that one could modify the results of an election much like a hacker's attack on any network IT system in use today. These attack attempts are detected all the time and are thwarted by diligent people with strict procedures and technology.

If one was able to get by the anti-intrusion procedures, it could be detected before or after the election and the appropriate remedial actions taken. While the Red Team takes the liberty to define an effective attack as including one that will affect the outcome of an election regardless of the fact that the attack will be detected, the goal is so frequently postulated on the Internet of election hackers is to do and not be detected. Since the Red Team's attacks are not claimed to be undetectable, one can only conclude that they fell short of that goal, too.

Without a full and complete analysis with recommended alternative courses of actions, including assessments of the security, accuracy, reliability, and accessibility, no action beyond additional recommendations and procedures should be taken based on this exercise. Thank you.

MODERATOR PÉREZ: Thank you.

We have Wayne Beckham, followed by Dan Ashby and Brett Garrett.

MR. BECKHAM: I guess we're the die hards.

My name is Wayne Beckham. For the last seven years, I've worked for the Riverside County Information Security Office, a former police officer and military veteran. I majored in information systems engineering at

California Baptist University. I'm a Microsoft certified systems engineer and a certified information systems security professional. Have more than 20 years in the information technology career field.

It will shock you to know that I have problems with the methodology that the Red Team used and looking at the security of the systems that were there. My particular comments today are directed at the U.C. Red Team's report on Sequoia voting systems.

My major issue with the methodology of the report is I went to great lengths to look only at the technology, not the surrounding policies and procedures. As a consequence, by refusing to look at the voting systems holistically, including the policies and procedures that actually make up the bulk of election management, they essentially put these systems into a no win scenario. Why a no win scenario? Well, Dr. Bishop talked about the analogy of a car. But the problem with using that analogy for the Red Team is that a car as he described it is a complete system. It's got everything it needs to be a car.

What Dr. Bishop was given was not a complete system. He had a portion of the system. The car he was given didn't have a LoJack, didn't have a Club on the steering wheel. I'm not sure it had windows or doors. He was given an engine block and told to examine it and to see what would keep this particular engine from being stolen.

So having been given that and seeing that there are none of the normal safeguards that you associate with a car, what else could he report to his hypothetical police officer except this thing is a death trap. We have no business using it on the highways. And after all, horses have been around longer, so let's use those. They're green friendly. That's a no win scenario that worries me.

Over the years, I've conducted a number of penetration tests. In none of them did the target tell me they're going to take down the fire wall, disable their D&D, and send all their technical staff on vacation for as long as I wanted. In other words -- and this has been pointed out before, for every Red Team I was a member of, there was a blue team looking out for me. And to me, that's the big picture that these reports missed. They're not macroscopic, they're microscopic. They zeroed in on the engine block and didn't see the highway patrol looking out for them. And there he is.

If the current systems are decertified, what will take their place? Are we going to continue to run with another series of Red Team scenarios matching the same high bar that has been set until we find a perfectly accurate, perfectly reliable, and perfectly accessible voting system that's perfectly secure? Well, Dr. Bishop's already told us there's no such thing. But we can get as close as humanly possible.

While the system vendors may not look at it this way, I think they owe the Secretary and the staff a debt of thanks. You've done a lot of groundwork for them. I'm sure even as we speak, they have teams of very talented people that are looking to address the legitimate issues that may have been raised in these various reports.

In the mean time, registrar offices all over this state are continuing to implement the procedural safeguards to ensure that there's never been a documented case of electoral fraud involving these systems anywhere in California. Thank you.

MODERATOR PÉREZ: Thank you.

Dan Ashby, followed by Brett Garrett, and Ann West.

MR. ASHBY: Okay. Mr. President, I wouldn't mind if you held up a one minute sign to me at two and one to help me count down.

My name is Dan Ashby with the Election Defense Alliance and also with California Election Protection Network. I'd like to say we've been encountering a great deal of misdirection today, because the emphasis has been talking about the malfeasant voters trying to do what I would consider retail fraud and hacking in from outside, when by far the greater danger is the inside hacker. As a matter of fact, the greater danger is fraud built in at the factory. Fraud can be clashed into a firmware at frequent intervals. Uncertified software patches happen all the time. Upgrades sometimes are performed right in the middle of an election. I mean, this is documented time and time again. I'm not making this up.

There are endless cycles of hardware and software upgrades that go into the current system. They constantly defeat any effort of real security implementation. At any one time, voting systems are about two years behind the currently recognized security requirements. For example, they tested to 2002 standards. Those are widely regarded as being ancient and completely useless for computer security. So we haven't even caught up to the 2005 standards yet. But that's what this Red Team was based on.

We heard that there's an unrealistic scenario, because it's unfettered access. Again, I will say the people who have unfettered access are people who write the code and people who build the software and the firmware.

I will point out that the two largest voting companies in the country that control about 80 percent of vote are ES&S and Diebold, and they have a common software genealogy, and that includes three or four people convicted for computer embezzlement and fraud who wrote the programs. And to our knowledge, those programs are still active. And I'm speaking about the Diebold programs. But they have a common ancestry going back to the mid 80s when there was a concerted effort to buy up large numbers of small voting companies and turn them into the three or four models that control most of the voting today in this country, about 95 percent of the voting.

Okay. It's been said those systems are 100 percent accurate. Well, how would we know? When has there ever been a thorough hand count audit of any election? I would like to know.

The one percent manual tally that we have in California is statistically inaccurate, as any cursory study of the subject will convey. And that's why we really do need to consider some rapid moves up in quality assurance to something like a ten percent ballot counted, hand counted in the precinct on election night before those ballots leave the protected purview of the citizen observed election count. Once they are in the mix and being fed into the voter machines down in county central, there is no accounting for what's going on in those software cards.

And believe me, we should be talking about elections in terms of virus, because that's what we have as a perfect analogy with these hundreds of memory cards floating around with executable code which can change behavior of the underlying software system. This is not speculative. This is not theory. This was proven.

I'm going to read a few comments from my friend Tom Courbat who the people in Riverside certainly know. He's also a chair of Election Justice with Election Defense Alliance. And he wants to point out that he says please do not continue to base certification of voting systems by adding layers of requirements that counties are required to shore up the security of our symptoms. Because he points out that he's aware of the CACOs says that courts can side with Nora Bone's findings and continue to use the systems which are already federally qualified. That's remarkable disrespect for law and contempt of the voters. And I don't think they are likely to implement the kind of changes that we want to see without a firm hand from Secretary of State Bowen, which I applaud for doing what was necessary. Thank you.

MODERATOR PÉREZ: Thank you.

Now we have Brett Garrett, followed by Ann West, and Teresa Favuzzi.

MR. GARRETT: I'm Brett Garrett, a concerned citizen from Redwood City, San Mateo County. I thank Debra Bowen from the bottom of my heart and thank all of who you are working to ensure the integrity of our election.

I do understand the concerns about privacy and accessibility. But I don't want a system that is so private that even I don't know how I voted or how my vote was counted. And I don't think any disabled person wants that either. The voting process must be transparent and simple enough that ordinary people can understand how it works.

I did hear some of the registrars saying that the voting machines are performing with hundred percent accuracy. I don't see how anyone can know that. If there was a glitch somewhere and it was not detected, you wouldn't know it. I don't see how anyone can make a statement that there is 100 percent accuracy with full confidence. I hope it's true. But by making that statement, you lose credibility by making it as a blanket statement.

I believe that for the system to be simple enough for people to understand how it works, we need paper ballots for full transparency. I want to emphasize I make a distinction between paper ballots and machine generated paper trails. Paper trails have been shown to be frequently ignored by voters. And second, as a voter, I have no assurance that the paper trail that is printed is the same as what was counted in the machine.

I'm also concerned by comments by vendors in which they acknowledge deficiencies in the machines that were tested in the top to bottom review, but the vendors claim their newer versions correct these deficiencies. This could be an endless cycle that goes on forever and ever always requiring counties to purchase new equipment and still continuing to deny citizens the right to know how the votes were counted in the sense we can't see the code that's running inside these machines. Those vendors want to keep it private.

It is a fact that sometimes election results are disputed regardless of what technology is employed. For example, many citizens dispute the results of the recent Busby and Bilbray election in San Diego. And in that case, citizens were not able to accomplish a recount. And I'm not even sure if there's any valid data to recount, because it was done by voting machines.

Paper ballots would constitute a ballot record which could be understood by anybody and could be recounted by hand, if necessary. Democracy requires a voting system that people trust and understand. I have doubts about many of the recent elections. I do not trust the voting machines, and I'm not alone, as evidenced by the fact that we are having this discussion.

Please implement a transparent voting machine, one not only that people can trust, but people do trust, paper ballots. Thank you.

MODERATOR PÉREZ: Thank you.

And we have Ann West, followed by Teresa Favuzzi, and Michael Keenen.

MS. WEST: My name is Ann West from San Bruno, California. I'm going to read my notes here.

The statement from the gentleman of -- well, let me see if I can read my notes here.

The gentleman from Sequoia talked earlier today about a three-pronged approach to ensure security. However, he has not taken into account the fact that the three-pronged approach or system of cross checks is not really happening in the real world of elections. For example, some counties are refusing to do the one percent manual audit. Poll workers are ignoring and sometimes even pulling off the tamper proof tabs by accident. And then machines are going home as we know with poll workers in San Diego for two weeks and into the precincts at least one to two to three days before, which allows security to be breached.

Second, many speakers today have called for additional guidelines relating to security. I would like to suggest in this connection that because there is a known revolving door between election officials and vendors that the potential for undue influence and conflict of interest is a serious matter. For instance, there should be no whining and dining that occurs at the election center event every year, and there should be no participation in the advertisements for the companies. Some people even go on line, put their pictures on line for these companies.

And there should be no hiring of government election officials before -- I think it's a mandatory two-year period is up. But people are ignoring that. That needs to be -- additional guidelines relating to security should thus incorporate regulations to ensure that election officials at the state and county level are not profiting in any way from the purchase of specific machines. Thank you.

MODERATOR PÉREZ: Thank you.

We have Teresa Favuzzi, followed by Michael Keenen, and Joseph Holder.

Teresa Favuzzi is not here. Michael Keenen. And after Mr. Keenen, Joseph Holder.

MR. KEENEN: Hello. My name is Michael Keenen, a software engineer and concerned citizen.

DREs, voting, electronic voting, it's a hard thing to do. I recognize that. And you guys are in a hard position. There's a lot of money at stake.

But I'd like to reiterate the importance of a paper ballot. Because I come from a software background, I know how well it is to manipulate bits. That's what computers do well.

People have lost confidence in the voting system, and there's a lot of reasons for that. But I think one of the major factors, at least for me, is that when I touch a screen, I can't be sure that my vote is going to be counted. Because with a paper ballot, I can be sure that persists. But on the computer -- I thought about this a lot. There is practically no way to ensure that what you push on that screen comes out.

Now, you can have the paper receipts so you can check them. But a lot of times voters don't. And so what you have is you're counting the digital count. The digital count becomes the vote of record, and that can be manipulated.

So what I'd like to see is simply a system, a simpler system. Because the problem is complexity. Computers are hard, you know. Security is extraordinarily hard. And that's because of complexity. So to reduce the complexity going to paper ballots I think would solve a lot of problems and save a lot of money. And it would also help restore voter confidence.

I think that's really my point there. Thank you.

MODERATOR PÉREZ: Thank you very much.

Here's what we have, Joseph Holder's card. When Mr. Holder is done, I'm going to ask Professor Bishop to come back up. We have a few wrap-up questions for Professor Bishop. Then I have a few people whose names I called and did not respond. If they're in the room at that time, I'll hear their comments. Otherwise, we'll wrap up for the day.

So Mr. Holder.

MR. HOLDER: Before I start my time, I just want to say my comments are not directed at all registrar of voters or all election officials. It only applies to those that they might apply to.

MODERATOR PÉREZ: You're on your time now.

MR. HOLDER: Thank you.

President Eisenhower warned us of the dangers of the military industrial complex. After four years of activism and research, I can say the election industry presents an even greater danger to our republic, for it puts at risk the very foundation of our form of government, the right of the people to choose who shall govern them.

Today, our elections have become captured by vendors that care more about their bottom line than about the accuracy or security of our elections and to many local election officials that care more about the expediency and convenience and their self interest and their duty to the voter.

This review has shown just how fearful the election industry is of scrutiny and how incestuous the relationship is between vendors and election officials. The orchestrated campaign by both the vendors and local election officials attacking the Secretary's review is not just revealing, but outrageous. Shame on those election officials that have participated in these attacks.

During the last four years, we have repeatedly seen deliberate efforts by election officials to obstruct public oversight of our elections. That must end.

While I welcome this review, it is not a top to bottom review. A top to bottom review would include unannounced forensic inspections of actually deployed systems. This would determine what firmware/software are actually installed, what lines are actually connected, and what communication links and drivers are activated. It would include a review of recent election event and audit logs.

I'm very disturbed that L.A. County voting system was not examined. That county alone can determine the outcome of any statewide race or proposition.

After what I have experienced and observed over the last several years involving election officials and vendors, I do not trust the election industry as a whole. It is as self-serving as the military industrial complex.

Electronic voting is inherently vulnerable. No amount of procedures, seals, or locks can provide the degree of confidence that we as citizens demand. We must know that we are governed by the will of the majority, not the will of some hacker, fanatic, or incompetent programmer. Procedures are no better than implemented.

Given the fact that every examination of every electronic voting system by an independent team has shown its unfitness for its intended purpose, I ask the Secretary to decertify all electronic forms of voting. The attorney general can then investigate possible legal actions based upon fraudulent business practices by the vendors.

Local election officials must stop defending the interests of the industry and defend the interests of the voters instead. They must stop hiding the process if they are to restore our trust.

I want to thank Secretary Bowen for starting to review these voting systems. I would warn her there are people within the election division that have and will subvert her efforts.

Secretary Bowen was elected on the platform to restoring the voters' trust in the electoral system. Any election official who does not adopt that same principle should resign or be fired.

MODERATOR PÉREZ: Thank you.

Professor Bishop, if I could ask you to come forward, please. We're going to take just a few minutes, if you'll indulge us, to ask a few more clarifying questions. But just as this morning's questions from the Panel were not intended to be a debate about the underlying issues of the report, just clarifying questions with respect to your presentation. The same for this afternoon's questions. So who would like to start with questions for Professor Bishop.

PANEL MEMBER FINLEY: Thanks for sticking around for this purpose.

One of the registrars who spoke today indicated that in her view all of the Red Teams' attacks required unfettered access to the systems. Do you know if that's true for all of the attacks as to all of the systems?

MR. BISHOP: Can I ask a clarifying question? Unfettered access meaning acknowledge of the source code, knowledge of everything? That's there were --

MODERATOR PÉREZ: Before you do, I just want to make sure that we're going to be consistent. And so without respect to any comments that were made today by other people who gave testimony, if we can get to the underlying question, which is -- because I just want to be very consistent. This isn't with respect to anybody else's testimony, but with this issue in the report itself.

PANEL MEMBER FINLEY: That's just what called it to my attention. I apologize.

MR. BISHOP: The question was whether or not all of the attacks that were found to be successful required unlimited, unfettered access to the system, source code, and everything like that.

The answer was no, they did not. Some of the attacks required simply access to the box, to the voting machine.

PANEL MEMBER FINLEY: My next question is did the Red Teams conclude that all of the vulnerabilities they identified could be remedied by procedures or policies?

MR. BISHOP: The Red Teams did not examine the policies or procedures. So I'm not quite sure how to answer that.

Perhaps the best way would be to say that there were some that could be very easily remedied by what I would consider fairly obvious procedures. There are others that would require much more effort, possibly even requiring changes to the source code or to the systems.

But again, I want to emphasize that that was my personal answer, because the Red Teams did not examine the policies and procedures. Just want to be very clear about that.

PANEL MEMBER FINLEY: And did any of the Red Teams make findings as to vulnerabilities to viruses in the voting systems, to viral spread of malicious changes to parts of the system?

MR. BISHOP: Off the top of my head, I can't remember the answer to that. And I will explain exactly what I mean in private if you like. I don't remember whether or not anything was said in either of the reports.

MODERATOR PÉREZ: Any other questions from Professor Bishop? No.

Okay. Thank you very much, Professor.

A couple of housekeeping items. We have three individuals whose names I called that submitted cards who didn't respond when their names were called. I'm going to read through those names again. If any of them are here and would like to testify, I'll hear from them.

In addition to that, it's been brought to my attention that there was a separate notice to hold a hearing -- to listen to testimony with respect to the ES&S InkaVote plus system. And if anybody, regardless of whether they've spoken on the other systems, if they haven't spoken with respect to ES&S InkaVote and would like to speak on that, I would invite them to go outside now and fill out a card, and I will allow them to testify about that momentarily.

Okay. The three individuals whose names I called before who did not respond were Michael -- I believe the last name is Covey from NFBC. No.

Virginia Ontiveros from CCB. No.

Teresa Favuzzi from the California Foundation for Independent Living Centers. I guess I called your name when you were out of the room.

MS. FAVUZZI: Just when I had to go to another meeting.

MODERATOR PÉREZ: And you've been ceded an additional three minutes. So you have a total of six minutes.

MR. FAVUZZI: Thank you very much. Well, last, but not least, I'm representing the California Foundation for Independent Living Centers. I'm the Executive Director. And the Independent Living Centers serves about 350,000 people each year with multiple types of disabilities.

And, you know, we are extremely concerned with access to democracy. And we have involved Independent Living Centers across the state in providing individuals here to help test the systems, and we are very pleased with the reports that have been put out that an effort has been put forward to actually test the voting systems and the way they were. And we are not surprised at what was found in the accessibility report.

There are about 20 percent of Californians identified as having some sort of disability or functional limitation. Yet, we know that only 30 percent of people with disabilities are actually voting. And we believe that some of these issues are related to inaccessible voting machines and voting systems and inaccessible polling sites.

So we have over the years been working to increase the access to voting for people with disabilities. This is not new for us. But we want to be clear that access to these voting systems is very important to us. There's clearly a lot of -- there's a lot of improvements that need to be made. But de-certifying the voting systems as they are now is actually going back towards in terms of access for many people with disabilities.

So we are certainly not where we want to be. But we certainly don't want to go backwards in terms of paper. Because what we know absolutely is paper is not accessible to the full range of people with disabilities and is absolutely inaccessible for a large number of people with disabilities. So going backwards with the de-certification is absolutely not where we want to go.

And where we want to go is where you're already taking us in terms of the accessibility report, which is a really good beginning to looking at some of the real practical issues that people experience with electronic voting systems, a look at how they can be improved, and then, frankly, improving them. Thank you very much.

MODERATOR PÉREZ: Thank you.

I have two cards with respect to the InkaVote Plus system. I believe both of these individuals have spoken. You had nine minutes with respect to the other systems. So I just want to admonish them that in the three minutes they have that, they need to stay on topic with respect to InkaVote Plus. If we go back to the other discussion we had earlier, I'll rule them out of order and move on.

So the two speakers are Brent Turner and Jim Soper. So Mr. Turner.

MR. TURNER: Thank you, again. This is just regarding ES&S, which I understood was an appropriate conversation. Thank you.

In San Francisco, we saw the Board of Supervisors embrace the concept of open source and call for both ES&S and Sequoia to disclose their code. We were already standing in place with ES&S, and I think that's where we were right now.

Sequoia was given the opportunity to disclose their code. I think when we're talking about ES&S and the rest of the vendors, we have to realize that all these systems are exactly the same. So in analyzing ES&S, there's been no great technological advances in any of these systems that would render one better or worse than the others. So I think they're all just in that same pool. And in San Francisco specifically, we're proud to have stayed in place with ES&S until the results came out, which now they're out. So now all of a sudden it looks for San Francisco like we were in a better position just to stay in place with ES&S.

I think the issue that's raised by this is nearly that all these systems are the same. And again we applaud all your efforts. We realize that this conversation is completely surrounding the use of proprietary source code. And until we can get the lobbying efforts of Microsoft and others that are trying to keep open source out of the equation under control, we're not going to be able to continue this conversation. It seems like at this point we have to stipulate that these machines are broken and that the democracy is in jeopardy.

And I appreciate all your time. Thank you very much.

MODERATOR PÉREZ: Thank you.

Mr. Soper.

MR. SOPER: Thank you. I've had the opportunity to talk with people who observed what's going on in and what's been there. And it is the most complex ruling cluster, I'll call it that, I've seen. They have a home brewed micro-tally system, NTS, that's never been federally inspected. They have an InkaVote system. They have Diebold. And a year ago, they had 18 Dell computers hooked up to the network James II which had nothing to do with running the election.

Something's fishy going on there. I don't think any system should be used in California that does not go through this top to bottom review. And that includes NTS. That includes InkaVote, the whole ES&S system. If they're not going to do it, then you don't get certification.

That's all. Please check it before the largest county in the state votes on it, because nobody has.

MODERATOR PÉREZ: Thank you.

I want to thank everybody who participated today for taking part in this very important discussion.

I will tell you that when I was appointed to the Voting Modernization Board five years ago, and the registrars will know this, we expected that to be a process that would take six months, maybe a year at most. Five years, two Governors, and four Secretary of States later, we're still engaged in this discussion. And quite frankly, I think that the discussion that has been made today is tremendously important to the decision that the Secretary will be making by the end of the week.

And I appreciate everybody's cooperation and patience today in helping this panel and the Secretary have all the information necessary to make very informed decision about where to go from here.

So thank you all very much. With that, our hearing will now adjourn.

(Thereupon the Secretary of State's
public meeting adjourned at 4:52 p.m.)

CERTIFICATE OF REPORTER

I, TIFFANY C. KRAFT, a Certified Shorthand Reporter of the State of California, and Registered Professional Reporter, do hereby certify:

That I am a disinterested person herein; that the foregoing hearing was reported in shorthand by me, Tiffany C. Kraft, a Certified Shorthand Reporter of the State of California, and thereafter transcribed into typewriting.

I further certify that I am not of counsel or attorney for any of the parties to said hearing nor in any way interested in the outcome of said hearing.

IN WITNESS WHEREOF, I have hereunto set my hand this 1st day of August, 2007.

TIFFANY C. KRAFT, CSR, RPR
Certified Shorthand Reporter
License No. 12277

CERTIFICATE OF REPORTER

I, JAMES F. PETERS, a Certified Shorthand Reporter of the State of California, and Registered Professional Reporter, do hereby certify:

That I am a disinterested person herein; that the foregoing Secretary of State's public hearing was reported in shorthand by me, James F. Peters, a Certified Shorthand Reporter of the State of California, and thereafter transcribed into typewriting.

I further certify that I am not of counsel or attorney for any of the parties to said hearing nor in any way interested in the outcome of said hearing.

IN WITNESS WHEREOF, I have hereunto set my hand this 1st day of August, 2007.

JAMES F. PETERS, CSR, RPR
Certified Shorthand Reporter
License No. 10063