United States Election Assistance Commission

Public Meeting

Voting Integrity Advocates Roundtable Discussion

1225 New York Avenue, Suite 150

Washington, DC 20005

Held on Thursday, April 24, 2008

VERBATIM TRANSCRIPT

Voting Integrity Advocates Roundtable Participants List

Merle King (Moderator)
Executive Director, Center for Election Systems
Kennesaw State University

Rob Richie
FairVote

Dr. Rebecca Mercuri
Bradblog.com

John Washburn
Voters Unite

Lillie Coney
Electronic Privacy Information Center

Dr. Barbara Simons
Verified Voting

Zinelle October
National Association of Latino Elected & Appointed Officials

Lawrence Norden
Brennan Center

Mark Skall
National Institutes of Standards and Technology

Brian Hancock
Director, Testing and Certification
United States Election Assistance Commission

PUBLIC MEETING

VOTING INTEGRITY ADVOCATES ROUNDTABLE DISCUSSION

DR. KING:

Well good morning, everyone and welcome to the fifth roundtable discussion that the EAC has sponsored for the review of the 2007 draft of the VVSG. There's a couple of housekeeping things I'd like to address first, but first thing is first, I'd like to recognize Commissioner Rosemary Rodriguez who's joined us this morning. Good morning, Commissioner.

MS. RODRIGUEZ:

Good morning.

DR. KING:

And -- okay. And I guess one of the first orders of business is to talk about the microphones that we have here today. There are two microphones in front of you on the desk. The wireless microphone is for the house amplification system. And these, certainly feel free to pick these up. You may have to share them as we go around the table for discussion. The microphones that have the cable to them are for the transcription service and they are sufficiently sensitive that they don't have to be moved. So if you would, make sure that the house mike is close enough to you. And is that audible in the back? Okay, thank you.

The second order of business is asking everybody to mute their cell phones or their PDA's or whatever it is that you have that will make a noise when you least expect it. Thank you. I know everybody here appreciates that courtesy.

Again, welcome to this fifth roundtable regarding the draft of the 2007 VVSG. Prior roundtables have included discussion with security experts, voting system manufacturers, voting system testing labs, and usability and accessibility experts. And there are two additional roundtables after this one. And all of the discussion here today will be recorded by a transcriptionist and will be available at the EAC website in about ten working days. One thing that I will ask you as a courtesy to the transcriptionist, if you use acronyms, it's very important that he come back later and be able to identify what those things are so the first time through if you're talking about something like the VVSG, the Voluntary Voting System Guidelines, et cetera, if you would, if you have unique acronyms that would be very helpful.

What we hope to eliminate in today's discussion which we've allocated three hours this morning until noon and then an hour after lunch, what we hope to accomplish is discussion of how the proposed standard will enhance or hinder the development and implementation of the next generation of voting systems. And of course what we all recognize is that the VVSG and the program that administers the VVSG is really a vehicle towards an end. And the end is voting systems that are accurate, reliable, secure, accessible, and affordable. And so we always ask that we keep those goals in sight.

I'd like to begin our session this morning by asking each of you to introduce yourself, introduce your role in the organization that you represent, and then provide us a brief overview of the organization and the mission. And I think that will help all of us

better understand the different viewpoints that are at the table. And I'm going to skip over Brian for right now and Rebecca, if I could start with you and then we'll just work our way around the table.

DR. MERCURI:

Okay. Dr. Rebecca Mercuri. And I'm here today representing BradBlog.com, which is, it's a blog, it's an online news posting type of service. I'm not paid by them. I don't really have much in the way of affiliation with them, other than putting up occasional postings and occasionally being on the air if they have a radio show, that type of thing. But Brad Friedman who runs the blog could not make it and he asked me if I would attend.

So in that spirit, I'll tell you a little bit about BradBlog, just briefly, since I'm really not the founder or anything. But basically, a lot of what it focuses on is election integrity and publishing news items about elections, but also providing a forum for people to discuss things pertaining to elections, but that's not all it discusses. It has other political bents that it's interested in. But primarily, I mean, usually the top lead item is about elections.

So the reason why Brad was not able to attend was because he's dealing with the aftermath, as we anticipated, there would be an aftermath of the Pennsylvania election on Tuesday. And he posted, you know, dozens, if you check Bradblog.com, he posted dozens of sightings and, you know, things that -- incidents that happened. So that's the type of thing that he does. Brad also does a lot of advocacy work, as well as I do.

I've been involved in election integrity and researching as a research scientist, researching voting machines and, you know,

election systems, since 1989, so that's like almost 20 years now. It seems like a really long time, which it sort of is. So my background is as a technologist. And my objective today is to sort of try to wear both hats, which is unusual for me. So, I'll be talking in a technology sense but also from the standpoint of you know what people are looking at, in terms of -- as voters, you know, as advocates. So that's today's topic is voter advocacy so...

DR. KING:

Okay.

DR. MERCURI:

...I'll be speaking in that respect.

DR. KING:

Thank you very much. Before we go to Rob, I'd like to recognize Commissioner Donetta Davidson, who's joined us this morning. Good morning, Commissioner.

MS. DAVIDSON:

Good morning.

DR. KING:

Rob.

MR. RICHIE:

Will I -- if I speak naturally, I'll be heard?

DR. KING:

Yes.

MR. RICHIE:

Okay, great. Rob Richie, Executive Director of FairVote. And I wanted to -- I have been Executive Director for sixteen years of FairVote and our focus, generally, isn't the technology of voting

equipment and I'm going to defer to a lot of people around the table on a lot of the particulars that come up today. But what we work on, is ways that we think we can hold elections that better achieve the values of what many people think representative democracy should be about, about majority rule, about fair representation of political viewpoints, addressing the needs of racial minorities in voting rights cases, where there is a minority vote dilution. And in the course of that advocacy for systems like cumulative voting, for instant runoff voting, or preferential voting methods, it often bangs up against the fact that voting equipment isn't flexible enough to handle these voting methods.

And just to give a little background about why I think this is important and it should be an ongoing part of the discussion, is that you can have obviously scams in elections, you can have corruption in vote counting and that should never happen, but you can also have voting methods that just don't achieve the goals that I think a representative democracy should achieve. And when you have the shocking reality of more than two candidates running for a one-winner office, which actually, is not that unusual, you don't necessarily deliver a representative outcome if you only allow people to vote for one candidate.

And so, we can assume like, okay, well all of our elections are going to be a vote for one kind of system but that can result in elections that actually aren't representative and indeed most of the democracies don't have what's called, plurality voting, where someone could win when a majority of people oppose them, would have either majority runoff systems or instant runoff systems. And

what we come -- run into, is the basic problem of a jurisdiction deciding to go that direction and then its voting equipment not being able to handle it and then the voting equipment vendor kind of muddles through and it often creates more messes and more security issues. And we want to see the basic value, when you are listing values that we all should be supporting, of flexibility. Of somehow having secure systems that can be flexible enough to accommodate reasonable public interest goals.

So that when a city like San Francisco passes instant runoff voting, eighteen months before it's supposed to use it for mayor, it actually can proceed and use it for mayor, which they could not do. And so the voters having passed this, didn't get what they wanted for a long time. Minneapolis passed this with 65 percent of the vote in November 2006 and it's looking pretty, you know, it's going to be a tough battle to get them to have an election in November 2009, three years later, even with extremely well organized backers who are trying to get it implemented in the city and that's because we don't have a regime that kind of makes it easy for a jurisdiction to make that transition.

I wanted to acknowledge a couple people in the audience who have worked on my testimony. I hope people can take a look at that testimony, but Amy Ngai is here and she is sort of in some ways the more particular expert on our voting equipment issues. And then my son, Lucas Richie who is here, with take-your-child-to-work day and he is developing the expertise that I've always wanted so thank you for both being here. And thanks to all of you. I really look forward to this discussion.

DR. KING:

Yeah, thank you. Lillie.

MS. CONEY:

Hi. My name is Lillie Coney. I'm Associate Director of the Electronic Privacy Information Center. I'll also refer to our organization as EPIC. EPIC is -- was formed in 1994, specifically to look at privacy and civil liberties issues, constitutional values as they relate to technology and policy, whether it's private sector, government or technology.

EPIC formed a voting project to specifically look at the issues of voter privacy and transparency, while also looking at issues of security. The voting project is brought together, really a broad resource of technologists, policymakers, legal scholars, looking at issues specific to voters, ballot secrecy and voter privacy and technology, and security and transparency, auditability, all of the competing interests that have to take place within an election environment, while at the same time meeting the need of voters who cannot really, easily demographically describe, other than for the most part, they are eighteen years of age or older.

Our work at EPIC, not only looks at domestic issues but also international issues of elections, because of the fact that we are trying to move an election process that was about 100 years behind in technology and at the same time, others around the world are trying to do some of the same things we're doing here with varying levels of success, trying to look for ways to rethink the topics of security, privacy, accessibility, usability, transparency, in an environment that is not easily defined by other experiences or

technology and policy and practice, whether it's in economic, whether you're using transactional relationships between common every day purchases. We've seen this analogy set of, trying to compare that to voting. Voting is a very unique process that has -- that begs us to spend a lot more time defining each level of the process, so that we can work on the hard problems that are involved in trying to successfully build elections that deliver on the promise of democracy, one vote for each person.

I'd like to thank the Commission for taking the time to invite advocates to the table for this discussion. We appreciate the opportunity and look forward to the work that we'll do today. Thank you.

DR. KING:

Thank you, Lillie. Barbara.

DR. SIMONS:

Should I -- am I okay with the mikes?

MR. MASTERSON:

Yeah, if you want to slide your table mike forward there.

DR. SIMONS:

Is it this one?

MR. MASTERSON:

No, it's the one to the left. It's the flat black.

DR. KING:

The little flat back one.

DR. SIMONS:

This thing?

MS. MASTERSON:

Yeah. And it will pick you up just fine.

DR. SIMONS:

All right, okay. I was wondering what that was, okay. So I'm Barbara Simons. I'm a computer scientist. I am retired from IBM Research and I spent many years as a volunteer at Association for Computing Machinery, ACM, which is the largest and oldest by at least if you use the right adjectives. Professional Society for Computer Science and Computer Professionals Educational, I mean, we have -- I probably didn't get them all right. And I'm former President and I'm also the founder of USACM, which is the U.S. Public Policy Committee of ACM.

I typically, when I've testified I've worn my ACM hat, so this is the first time I've worn my Verified Voting hat. I am on the Board of Verified Voting Foundation. And Verified Voting started, well I'm not sure exactly when it started, but what kind of begin was, when David Dill, who's a Professor of Computer Science at Stanford, discovered to his horror that people were actually buying and voting on paperless computerized voting machines, which as a computer scientist he knew, we all knew were insecure. And then -- and so he put up a petition on his website to gather signatures of technologists, saying that this is a bad idea to have, to use these machines, which of course could not be audited post election.

And then we all -- then he discovered to his greater horror that Silicon Valley was about to buy some of these machines. And that's when I got involved. I joined David at one point, of lobbying political members of the Santa Clara County Board of Supervisors. A number of us PhD computer scientists went to long boring

meetings and sat through for three hours listening to everything and vendors making their pitches and then in the last few minutes, we were each given about a minute and a half to say why, from a technological perspective, these things were a bad idea. Needless to say we were ignored, except for a clause that was put into the contract saying that if paper trails were required, that the vendor would have to cover that. And California subsequently did require paper trails and the vendor did have to cover it, so I think we did Santa Clara County a big favor.

When we started off, we naively believed that all you had to do was to add a paper trail to a touch screen voting machine and that would suffice because it didn't occur to us that the vendors would deploy such poorly engineered technology to do these retrofits. Since then, I have to say that the view of Verified Voting Foundation and my view as well, is that these paper trails are not really very good technology. They're better than nothing but what really is far better is hand marked optical scan paper ballots, which are counted in the precinct by scanners, with precinct based optical scanners. That's the main technology that we feel should be deployed, together with statistically significant manual random audits.

I just -- just one final comment. This whole voting system has taken over my life in a way that I had no idea it would in 2003. And I know a lot of people have been sucked into it because the more you learn; sometimes the more horrified you become. And I have just written a book with Doug Jones on voting machines which

we hope will be coming out in January, so I urge you all to go buy it when it comes out. Thank you.

DR. KING:

Okay, thank you, Barbara. Zinelle.

MR. OCTOBER:

Hi, good morning. Zinelle October from the National Association of Latino Elected and Appointed Officials Educational Fund. We're an organization, non-profit, non-partisan who represents the over 6,000 elected, appointed officials, Latino officials throughout the United States. We focus on everything that would facilitate the participation of Latinos in the election process in general. So that's everything from immigration, naturalization, to registration for voting, to actually getting to the polls to vote, and then eventually to even run for office.

And so, like Rob, traditionally we haven't really been, the focus hasn't been technology for us, but realizing that voting is an important part of what we do. Increasingly, we've realized that we need to take a stand on voting technology, specifically of a policy analyst at NALEO. And I work on voting and election reforms in general in particular on how the voting technology affects the Latino community.

So that's kind of been our focus of late, my focus particularly, and that's why we're happy to be here. Thank you so much for having us. We look forward to the comments and participating, from advocate standpoint of course.

DR. KING:

Good, thank you. Larry.

MR. NORDEN:

Good morning. I'm Larry Norden. I'm from the Brennan Center at New York University Law School. The Brennan Center is a think tank and public interest law firm that was founded by the family and former law clerks of Justice Brennan, as a living memorial to Justice Brennan. We work on many issues, a number of democracy issues, including campaign finance reform and redistricting. And we do a lot of work in the area of voting. Our focus in the area of voting is on decreasing barriers to the vote, increasing voter participation, and ensuring fair, accurate, and reliable elections. I'm an attorney at the Brennan Center and I direct our voting technology project.

DR. KING:

Okay, thank you, Larry. John.

MR. WASHBURN:

My name is John Washburn and I'm representing Voters Unite today, which is an organization, founded by Ellen Theisen and John Gideon. And their primary focus has been just to report on, you know, voting technology, primarily with the focus on voting technology. Their probably two greatest resources that they provide is a daily feed of news stories. It's the Daily Voting News, which Mr. Gideon produces and then the documentation of known failures of voting equipment, dating back, I believe to 2003, sorted by vendor, type of failure, date, election, various categories.

The reason they asked me is, the topic is relatively technical and I've been a software tester since 1994. And my particular interest, when it comes to the intersection of voting machine, is the

testing and certification process, so I've made some comments on that in the past. And at the urging of -- well I wouldn't say urging, the -- at the prompting of the Wisconsin State Elections Board, I've actually written a guideline on how to do your pre-election functional testing. So if there's any election officials who would like to do that job well, there are standards available. And if you want, they're distilled to one page, five simple rules for testing voting equipment.

And I guess that's -- the one thing I would mention in -- that came up with -- as I was discussing with Ms. Theisen how to decide this is, as a country, we have not debated fundamental questions about voting, since the 1890's and 1900's when we decided to adopt the Australian ballot, which is what most of us are familiar with. And because of that, we don't really have as a body politic a good consensus of what constitutes a successful election. And until we even have a rough consensus as to what that is, picking a piece of technology is a poor -- it's putting the cart before the horse, literally, because as an engineer, it's very difficult to design a successful solution if you're uncertain what the exact problem is.

So that would be the more overarching theme with Voters Unite, is that some of these technology questions are made well in advance of any consensus on what they ought to do. Aside from the reliability, most of them are poorly implemented. Even if they were well implemented, I suspect they would be failures to many people because we don't have a consensus of what they ought to do so.

DR. KING:

Okay.

MR. WASHBURN:

And as a tester, I'm fascinated with the question of what ought it do?

DR. KING:

Well I'm fascinated with the concept of a one page document that deals with voting.

MR. WASHBURN:

It took awhile.

DR. KING:

I'd like to recognize Tom Wilkey, Executive Director of the EAC has joined us this morning. Good morning. Mark.

MR. SKALL:

Good morning. My name is Mark Skall from NIST, the National Institute of Standards & Technology. I have been involved in previous roundtables, all but one. In a way, I almost feel like Barack Obama or Hillary Clinton, that this is yet another debate but just like those debates, I think you do learn something at each debate and I've certainly learned from the previous roundtables. So I think these are very useful and I want to thank Merle, and Brian, and Matt for holding this and also for putting me in the same seat because I do get confused if I have to change seats.

NIST's role is to essentially advance the competitiveness of U.S. industry, through our measurements and standards. We do this in many different arenas, many different disciplines. I'm particularly involved in the IT world. My role is the Division Chief of the Software and Systems Division and we have a long history of

helping develop standards in IT, dating back before some of you were probably born, writing test sweeps. We got involved in voting because of HAVA, which was a natural fit for us to help develop standards in test sweeps.

DR. KING:

Okay, thank you, Mark. Brian.

MR. HANCOCK:

Thank you, Merle. Like Mark, I've been at all these roundtables, sitting in the same seat and I guess we can flip a coin to see who's Barrack and who's Hillary and we'll do that at the break. In any case, on behalf of the EAC Commissioners, our Executive Director, Tom Wilkey, let me welcome you and thank you for coming this morning. As Merle noted earlier, this is the fifth in our series of roundtable discussions. We'll actually have two more of these sessions. Tomorrow, in this very room we have a roundtable discussion with election officials. And on May 5, again here at the EAC offices, we're going to have an interdisciplinary roundtable that's going to be comprised of individuals from all of the areas in which we've had roundtables up to this point. So again, that's May 5.

In order to accommodate the discussions we've had and to receive public comment on these discussions, the EAC as you know, has extended its public comment period on the Draft VVSG until May 5. And certainly, for those of you that have not yet commented, we do encourage you to do so and make note of that May 5 date.

Again, these roundtables would not be possible, as you all know, certainly all the participants know, without the great work that Matt Masterson has done, so I want to acknowledge Matt, thank you very much. And before I kick it back to the very capable hands of our moderator here, I just want to reiterate the statement that I've made at all the other roundtables, as to the purpose for the EAC holding these discussions.

We certainly, of course first and foremost, want input and comments on the Draft VVSG, but these comments are really only a means to our end goal of developing and implementing the most robust set of standards possible in order to make voting systems more secure, reliable, accurate, and accessible. You know it's pretty simple to say those are sort of the baseball and apple pie concepts when we talk about them but as you all know, they're very difficult to put into practice.

By undertaking the development and adoption of this new iteration of the VVSG, the EAC and its partners are certainly charting the course for the development of voting systems for the foreseeable future. It's certainly an awesome responsibility and one in which we are undertaking with full commitment and proper due diligence. The excellent work of NIST and the TGDC in putting this document together is only the beginning of the process. The real work of the EAC and its partners in this effort and the American public begins now.

The questions we pose to you as conversation starters today relate to some of the very fundamental aspects of the TGDC draft document. The questions are asked so we continue in the open

and reasoned discussion that we began in Austin last December at the very first roundtable and again to look at the direction we're headed. We're charting the future of our voting systems.

As has been the case with all of our panels up to this point, we have a very distinguished group of panelists here today. And everyone certainly has a number of views and opinions to express. All of these certainly have merit and we take them gratefully. We should remember though that we only have a limited period of time and in order to make the best use of that time we should try to focus as much as possible our efforts on the document at hand which is the Draft VVSG.

But again, thank you very much and we appreciate you coming today and look forward to an excellent discussion. Merle.

DR. KING:

Good. Thank you, Brian. And I'm Merle King. And it is my pleasure to be moderator of this panel. I would like to go over just a few ground rules that will help us expedite the work that's ahead of us. One is when you wish to be recognized, if you would put your tent up on end and that helps me keep track of who would like to speak and in what order. Do a little math, we've got nine panelists, we got six questions, we got three hours, so self regulate. So, as we start to move towards our first break at 12:00 -- or at 10:30 and a lunch break at noon, my job will be to help us keep on task and try to get through these six questions that the EAC has identified as really being important points to resolve as they move forward on ultimately what will be their decision on the status of the VVSG. We'll take a break at noon and when we return from lunch

at 1:00, we'll have a summary opportunity and we'll go around the table and each member of the panel will be given time to summarize any points that they felt really needed to be emphasized to address any issue that came up in a prior question that they've thought about over lunch that they would go on record. And that's an opportunity to really make sure that whatever you think is important out of this discussion today that you have an opportunity to drill down through that and in one sense get the last word in that regard.

The -- for those of you who have submitted written documents, thank you for that and they're out in the lobby. To that end, if you have submitted a written document that will go into the record and no need to read from it during the panel discussion. So if you have submitted written testimony rest assured that that will find its way into the record.

As a way of motivating each question, what we realize and I think Zinelle kind of addressed it eloquently in her opening remark, is that not everybody at the table has the same amount of exposure to every issue that's represented in these questions. And what we've asked is that members of the panel or myself will introduce a question to kind of help put it into the context. And Rebecca has offered to introduce Question #2 and Lillie Question #5 and I'll do the remainder. I'm sorry, Mark's going to do Question #3 and I'll do the remainder of them. So at each question, we kind of like to ramp up into it. And then we'll work our way around the table and try to get everybody's input into it and at some point again keep in mind that we're trying to move through all six questions and we'll move

onto the next question recognizing that each of us will have an opportunity after lunch to come back if there's something that you felt was unsaid or needs to be restated about a question that we dealt with earlier.

Okay, so Matt, can you put the first question up, please? At the very first roundtable discussion that we held in Austin with security experts, the issue of risk assessment came up. And risk can be described as a threat to the continuity and performance of a system. Every system has processes that are designed to transform the inputs of that system and the outputs and then controls that ensure that the processes are working properly. Often discussion of voting systems does involve discussion of risk and very frequently those risks are stated in very broad terms and they are not hierarchical. A common way, in commercial systems, is that we look at the probability of a risk occurring and we multiply it by the dollar consequence of that event and that gives a way of prioritizing risk. Well, I think what we all recognize is, that voting systems don't have outputs that equivocate in the same sense that commercial systems do. Voting systems have unique properties that cannot be expressed in dollars necessarily.

At earlier roundtables, participants discussed how the absence of a formal assessment of voting system risk makes it difficult to prioritize the application of limited resources, to address the risk and it also impacts the ability to identify appropriate tradeoffs. That, if we can't have everything, what's more important than another thing? So, risk assessment can be wide ranging in the scope, some elements are also, somewhat, counter intuitive so

if we work in elections we know that one of the risks that we face is, inadequately trained poll workers. And so when you're designing voting systems, how do you address that particular risk into the design of voting systems? And I bring that up to say, that not all assessment of risk and then carrying forward that risk assessment into the design and the testing criteria is a straightforward process.

So, with that, if I can read from the question that's hopefully right behind me. On October 7, right, 2005, NIST held a risk assessment workshop. The results of the workshop were, at the site specified there. In doing so, NIST recognized the importance of evaluating threats when developing secure voting systems but no formal risk assessment has yet been developed. The EAC is now interested in learning how to best develop a risk assessment framework to provide context for evaluating the security implications of using various technology.

So the first question that we pose to the panel is, what are some of the essential elements of a risk assessment of voting systems? And if we can start with that one, then we move onto the other two, which, I think are also up there.

DR. MERCURI:

Are we just going to go around?

DR. KING:

Is -- not everybody is probably going to want to talk on every topic but if this is one that you'd like to kick off on, put the tent up, that will help me identify the order. And I have Rebecca, then John, then Larry, and then Barbara. So Rebecca.

DR. MERCURI:

Okay. With regard to just the essential elements of a risk assessment, first of all, I was sort of surprised to see this question, especially considering the NIST involvement with the EAC and in development of the TGDC and, you know, the VVSG, so there's all those acronyms out there, sorry about that. But the reason why I was surprised was because there -- this is a -- there are industry standard ways of doing this. Creating a risk assessment is, you know, one could say, it is rocket science, but it definitely is something that we have formats and parameters for doing.

And in particular, there is a format which the NIST used to administer which was called the common criteria. That particular program is actually an international program and it's now administered under the Common Criteria Recognition Agreement, so you can look it up on the internet, just as common criteria, you'll find commoncriteriaportal.org and that's the current administration of the common criteria.

And in the common criteria, basically what it is, it's an internationally recognized program for security assessment. And there's also a, you know, there's a technology, information technology security evaluation, which is known as the common criteria and there's also a methodology for information security of evaluation, which is abbreviated CEM. It's, as I say, it's not new. I personally have been recommending that this be applied since 2000 and its predecessor, which used to be referred to as the Rainbow Series or Orange Book. That was also administered, that program was administered under NIST. I was recommending that back in the 90's. Although it's not new, it is considered the best

generally recognized security program in the information technology industry. And it does specify such things as, how to go about proceeding with creating a risk assessment and how to mitigate those risks.

So, I guess that's why I'm sort of surprised. I mean, certainly we could detail those essential elements but they're embodied in the 500 or so pages of the common criteria and there they are. So, you know, why voting has not been applied to this program, there's a multitude of reasons I'm sure, but it's certainly not required in this industry. It is required in certain other industries. And some industries have made it a requirement, sort of a voluntary requirement, like the healthcare industry. It's required for use in many military applications. And so, this is something that's available. It's something that we could do and, you know, there's no reason why we shouldn't proceed with it.

So, you know, that's my answer to the essential elements. There they are, look them up, and apply them, essentially.

DR. KING:

Okay, thank you. John.

MR. WASHBURN:

Well, the first thing with the risk assessment I would ask is, which risk do you want to assess? With a software system, there is two essential kinds of risk, one from what I call, a mistake and one from malice. One is, the system has faulted in some way, which gets into a whole reliability engineering and the other is, is that it's been deliberately manipulated to enter a fault state of some sort, you know, to some purpose.

For a mistake, again, we have well-established standards for reliability assessments. You know doing a failure mode analysis, things along those lines. Again, they're well established in the healthcare and avionics industry, how to perform such a fault mode analysis. And for malice, again the common criteria and they came out of the, I don't want to say industry but certainly out of the community which, you know, with the national intelligence community, that definitely was assessing the risk of things that was very hard to attach a dollar amount to. I mean how much does it cost if you don't discover a spy? I mean, that's not something you put a real crisp dollar figure to. So it's not like the common criteria are unfamiliar with the idea that there are non -- that there are risks that have -- risks that are quantified in something other than dollars.

So again, it's the -- there's two different methodologies, whether you want to mitigate or do your risk assessment for mistake or malice. And with elections and the voting technology, I often joke that any system that offers sex, power, or money as a reward, some participants within that system will cheat to get that reward. And elections can get you any little string, any combination you want. So, to overlook insider risk and focus on poll workers and voters, seems to miss the largest risk when it comes to malice.

DR. KING:

Okay, thank you. Larry and then Barbara.

MR. NORDEN:

Well, the Brennan Center is certainly happy to see the EAC interested in this subject. As some people may know, the Brennan Center, working with many of the countries leading security experts

and technology experts and election officials, actually used the work collected at NIST's risk assessment workshop to do a threat analysis on the nation's voting machines.

I would echo some of what John said. I think key in doing a threat analysis, in doing a risk assessment, is what are you looking to assess? There's -- there are -- there -- you could be looking at a mistake, you could be looking attacks against the system. And also are you looking -- are you attempting to assess what kinds of attacks or mistakes might, for instance, might shake public confidence? Are you looking at what might change the results of a statewide election or a national election? Are you looking at what kinds of mistakes might go undetected, as opposed to mistakes that could be corrected? It seems to me that you could do many types of these analyses.

One thing I would say is, while I'm very happy that the EAC is interested in this and I think it could be useful to election officials in developing procedures and in gaining an understanding on how they should use these machines, I would hope that pursuing risk assessments would not delay the implementation of the next iteration of the VVSG.

And, you know, we do have, we certainly have a pretty good historical record of the types of mistakes that occur in using these voting machines and their repercussions. And, in addition to doing any kind of risk assessment, I think it's important to look at problems that we've had with these machines in -- and I think that has been done to a larger sense in the Draft VVSG, but certainly

also in developing procedures for using the machines for election officials.

One thing I would emphasize about a risk assessment, is that, not all risks are created equal. In the Brennan Center's risk assessment, we've looked at the kinds of undetected attacks that could affect the outcome of a statewide election and I would say that's probably one of the -- as far as I can imagine, one of the highest negative impacts that I could imagine on an election system. And what we found in that risk assessment was that for that type of threat, the insertion of corrupt software were among the least difficult of attacks that we looked at. And again, this was in large part using the work that came out of the risk assessment workshop, although certainly we developed other work through working with election officials and these security experts.

My understanding is that where -- even where you're talking about a relatively low risk of some kind of attack happening, where the impact is especially negative and high, that regardless of the facts that we may see these attacks as relatively low risk, there's an understanding in the security community and at NIST, in other contexts, that you have to take certain minimum security steps, no matter what. And I would emphasize that fact to the EAC as well.

DR. KING:

Good. Thank you, Larry. Barbara and then Mark.

DR. SIMONS:

Well, some of what I was going to say has already been said, so I second a lot of what was said before me but I have a few things I thought I would add.

In our written statement, we took a crack at coming up with some questions that one might ask about risk assessment and to some extent, they're repetitive to what has been said already, but basically looking at the security properties, potential attackers, baseline of possible attacks, defenses, assumptions about procedures, which I think is an important thing I mean one might -- you have to -- one question for example is, if you're depending upon poll workers to execute certain procedures to prevent or to work against a particular risk, how do you know that they'll always do that? And how do you quantify risks? Obviously quantifying them is going to be very hard. As Larry said, the stakes can -- you can have a very low risk event but with incredibly high costs. For example, outside of the voting realm, the risk of a nuclear weapon being set off accidentally and demolishing an American city, hopefully the probability is very low, but if that were to happen, it would be devastating. So you have to basically compute expectation and those things.

And a point, which I think we sometimes lose track of, is that voting is really a national security issue. And I think we really have to treat voting the same way we would treat other major national security issues, which is one reason why I get really upset whenever I hear people talking about glitches in voting machines because a glitch might -- we don't know. I mean, a glitch is a way of downplaying problems. Problems could have major repercussions. So, on the one hand, we have to get a handle on managing risks. I think that's an important thing to do and I do hope the EAC will consult with the technological community, with

people who have experience in risk assessment and develop some additional standards in this area. But on the other hand, we have to acknowledge that there is no way we can be completely risk free in this area.

Given that we cannot eliminate all risks, we have to think about alternative methods well. In particular, we need to be able to audit the results of elections after the elections happen, before it is certified, because we just can have no guarantee that an election has not been either manipulated or falsely reported because of software bugs or something else.

DR. KING:

Okay, thank you, Barb. Mark and then John.

MR. SKALL:

Yeah, I think trying to conduct a risk assessment is a very worthy go. I applaud the EAC for doing this. Let me just give a couple of caveats along the way. I think Merle hit the nail on the head when he introduced this subject. By the very nature of risk assessment, there are many, many subjective analyses in here. And just because there are ways in other systems, treated subjectivity doesn't necessarily mean that the outcome is not necessarily just as subjective as the input. So the example Merle gave, assigning a probability is very difficult of a threat occurring and assigning the magnitude of the loss. For instance, in voting, the undermining of democracy, the undermining of the system that is a potential loss and it's obviously impossible to specify a dollar amount on that.

We think we made a really good start in the threat assessment workshop at NIST. One of the things we found out is,

it was difficult for us to go to the next step. Our goal was to try to come up with probabilities, or at least ranking the probability on various threats. We found that you really need a mix of disciplines involved. And I think at that workshop we didn't have enough voting officials. We didn't have enough vendors. We really need different people looking at different parts of the problem. Unless you have that, it's even more subjective.

To do a good risk assessment, as been stated before, it needs to be very thorough, it needs to take a lot of time. That may, in fact, delay things and I am also a little bit worried about that. Of course the alternative of doing it, sort of half-baked is, that you don't get output. So you really are faced with this dilemma. It's a worthy goal but there are a lot of challenges in trying to actually affect the goal.

DR. KING:

Okay, thank you, Mark. John and then Rob.

MR. WASHBURN:

Yeah, just a quick addition is, also with risk assessment, one of the goals when you try to mitigate a risk is you -- is notification sufficient or do you actually want to block the occurrence of the risk? Right now, I would argue many of our voting systems even failed the notification. They don't fault well and tell you that they faulted well and a good example would be the Congressional District 13 race in Florida. Currently, we have a supervisor of elections who says that, well people came in they just didn't vote and we have a candidate who contested, no, we think the machine lost the votes. Yet the machine has so little evidence, it doesn't let

you answer the question, so that that risk is kind of undermined in confidence, if it at least would notify better. So, what I wanted to add was, that one of the outcomes of risk assessment is, how do you mitigate the risk or accept it? You have two possibilities. You can block it or at least notify. And I would argue that we should consider, if nothing else, notify.

DR. KING:

Thank you. Rob.

MR. RICHIE:

I wanted to make a brief comment again, through the lens of our work on researching and promoting different voting methods, because through that lens we obviously will run into these issues. For an instant runoff election, a rank choice ballot for an optical scan counting system, the essential thing it needs to do, is capture the ballot image of each voter's ballot, because the information on that ballot needs to be used in the algorithm of doing the count. And what we found was, actually a lot of optical scan systems don't capture ballot images. And as we looked into that more and sort of thought about that fact, what that means is, that after an optical scan ballot is counted that it's -- then, if there's something that happens to the ballot, there's no sort of redundant way to see that maybe something happened to the ballot.

So it seemed like a reasonable proposal to say, well it's a good issue to have sort of a redundant record of a vote, if it can be captured at the time that the voter's casting it. But then that raises issues of, what then becomes the audit trail. You know, if you use

actually the redundant image or do you use the ballot itself and would there be controversy over that.

So that, I guess the point I wanted to highlight is that, there is an issue of how to create procedures that anticipate risk, like the risk of paper ballots being destroyed or, either accidentally or maliciously, how it would change. And then figuring out procedures on how to say, deal with this issue of, what becomes the audit trail. I also think again, with this sort of flexibility point, that it's something like a rank choice ballot, which again, a lot of other countries are using and is, you know, not getting a lot of interest in the United States, is used. It creates different issues to evaluate risk. So that again, that flexibility to anticipate potential development in our process, so we don't just look backwards but look forwards and again, what needs to happen with our rank choice system is that, the ballot totals need to be aggregated and then that leads to -- the algorithm accounting needs to then, you know, the other ballots are handled in certain ways, so that information needs to be aggregated and then worked on, doing a count. And that might rank different things to be looked at than just the totaling of ballots, so again kind of looking at that broader picture.

DR. KING:

Okay, thank you, Rob. I wanted to follow up on something that Barbara mentioned in her response and that is, is it possible that we can audit all risk out of system? I think Barbara said we can't.

DR. SIMONS:

No, I didn't mean all the risks.

DR. KING:

Right, right, well I think you said that, we can't audit all risk and so the prioritization of risk can give us guidelines as to where we can allocate the resources. And I bring up an example. What we know in my State of Georgia, in the upcoming primary, there's going to be between 300 and 400 voters out of 5.6 million that are not assigned to a precinct. Now that's because of dirty data in the VR System. So, we know that there is a potential for 400 voters or so to be disenfranchised. That is a very, very high probability of that. But that's not the kind of risk that I normally, here, discuss. I usually here for lack of a better term the kind of sexy risk issues, the cloak and dagger stuff, the insider attack. And I think Mark also highlighted in his comments, about the need to have a multi-disciplinary viewpoint on the risk assessment.

So, going back to my initial question, auditing all risks out of a system, are there opportunity costs associated with that? And how might we guide the EAC in prioritization of risk? And I think I had Lillie first, and then Barbara, and the Rebecca.

MS. CONEY:

I'm glad that this discussion is happening around this table with advocates because this is a very difficult political discussion to actually have in the clear and not behind closed doors or email.

DR. KING:

There we go, thank you, Barb.

MS. CONEY:

I'm sorry. This is, I was saying that this is a difficult political discussion to have in the clear because you're acknowledging part of the discussion of risk are losses, acceptable losses.

DR. KING:

Um-hum.

MS. CONEY:

And being able to create a matrix around that that's communicated not just to elections officials but to the broader public. If you have X amount of elections over the course of the year, then you have a 3 percent error rate of reported outcomes. Is that an acceptable level of bad outcomes for an election? And being able to say that we can acknowledge we won't have 100 percent effective elections out there, but quantifying acceptable losses is going to be a hard political discussion but one that needs to take place in the realistic application of how elections happen and getting away from the fault, focusing on fault, or blaming...

DR. KING:

Um-hum.

MR. SKALL:

...people in the outcome. But if you don't quantify, you can't really work on those hard problems and start to reduce those acceptable losses and get as close as possible to perfection as you can get.

One other thing I'd like to add. Dr. Peter Neumann, who is Chair of the National Committee for Voting Integrity or the EPIC project that I work with, is a principal scientist at SRI Computer Science Lab. He also moderates the ACM forum on risk. I think it's very informative and I'd like to be able to include something in the material for this discussion on that.

DR. KING:

Thank you. Barbara and then Rebecca.

DR. SIMONS:

When I talked about auditing with respect to risk, obviously I didn't mean -- there's many things we can't audit out.

DR. KING:

Um-hum.

DR. SIMONS:

I really had in mind addressing issues like wholesale election fraud, which is one of the reasons I think why a number of computer scientists have gotten involved with the whole issue of computerized voting machines because we realize that if it's -- if an insider for example -- our initial response, thought was, if an insider can insert malicious code into the software of one of the major vendors, that could have such a huge impact that basically one or two individuals could change the outcome of a presidential election and that seems pretty scary, I think, by anybody's standards.

Obviously, there are many different kinds of risks. You mentioned some others that we have to worry about and auditing can't address them all. It can't address, for example, some of the risks that I think we're going to encounter with the electronic poll books, where people are going to go to vote and find that their names aren't on these electronic poll books because of problems with dealing with database.

So, but I do think that audit plays a very important role in as much as, convincing the public that the person who was declared the winner of a race, was in fact the winner. And so long as people don't trust the outcome of a race, and so long as they question the outcome of a race, feel that the wrong person one, feel that the

race was stolen using some of the conventional methods and, again, there are many ways one can steal a race and you don't have to do wholesale fraud to steal very close elections, but at least if we can convince them that the machine count, whatever kinds of machines you use, that the count was in fact correct in choosing the winner. And if we can make that statement with 99 percent confidence, I think that's going to go a long way towards bringing back the belief in the whole electoral process. Because I think that some of the events of the past decade have seriously damaged that. So, but audits can only go so far. There are many other issues that we have to deal with which can't be dealt with by audits.

DR. KING:

Okay, thank you, Barbara. Rebecca and then Larry.

DR. MERCURI:

Since you, you know, you're bringing up this sort of weighing of risks and from a computer science and a mathematical standpoint, let me reiterate what you had started earlier. The recognition of all possible risks is theoretically impossible. So, that's just known in the computer science literature, except in infinite time. So you're not going to have an election running in infinite time so it's just theoretically impossible. So there's no way to ever get that 100 percent confidence that all risks have been mitigated. But yet, we still want to say to the public that every vote is going to count, even though we well know in the voting industry that every vote never does count. It's -- that -- this is just a known thing. It used to be a dirty secret before 2000 and now a lot more people know about it.

So the problem really is, how are you going to weigh these different types of things that you're going to mitigate and how are you going to establish values to them? And again, I go back to the common criteria not that I'm, you know, hawking it for any particular reason. But the common criteria program establishes what they call evaluation assurance levels. They're called EAL's. And basically you say how critical is this component of the entire product? And then you establish a level and then you say you have to satisfy this minimum level and some components might have to satisfy something even higher than that. And I'll give some examples. There are operating systems that have passed through EAL 4. EAL 4 is probably the minimum level and I have assessed this. It's in my writing. It's actually in my doctoral dissertation. The EAL 4 level does address most of the needs of a voting system, so you might want to look at that.

But for example, some modules like cryptography and you've heard a lot of cryptography bandied about in the voting arena, that we could use cryptographic voting and somehow that would be more secure. Cryptography is generally understood that it has to actually be assessed at the EAL 7 level, which is the highest level. And I don't believe that there are any products that have satisfied that yet. An EAL 7 requires mathematical provability. If you're going to use cryptography, then you're using math and you're implementing an algorithm or a formula and you have to determine that that algorithm or formula has actually been implemented correctly. And the only way you can do that is through mathematical provability.

Now the cryptographic community and I have addressed -- many of the cryptographers know me very well because when they say, you know, I've got this scheme; I go, well prove it. Show me the math. Give me the math. And as scientists, we're required to do that, but unfortunately in voting we don't actually see that happening, where people are actually required to prove that their formula for cryptography and cryptographic projection of voting, actually is correct. So I mean, that's the type of thing that I'm looking at when trying to assess this.

But I'd like to also just add one other aside. We're losing track of the voter. Remember this is a voter advocate type of discussion. And it's not just the risks in terms of, okay, mathematically we prove that cryptography, you know, this cryptographic algorithm is wonderful, but how are you going to convince the public of that? Most of the public doesn't know anything about cryptography. I would say, most of the people in this room not to insult anyone, but I suspect most of the people in this room do not know a lot about cryptography. And how are you going to overcome the voter perception that elections are inherently corrupt and yeah, you can waive this cryptographic thing and all your gurus approved of it but I don't see that it's actually doing anything for me and now everything's all gobbledy-goop, it's all been encrypted, so I can't even check it.

So those types of things and plus the insider risks. The VVSG, we're looking track of what we're talking about, is this VVSG Draft. This VVSG Draft as well as all of the other VVSG's before it failed to take insider risks into sufficient consideration. And you

had mentioned this, John earlier. And that is a critical component because if you have the majority of the public. Maybe not the majority, but a significant percentage of maybe millions of people in the public, saying that we believe elections are corrupt and you have this enormous VVSG that you've never really addressed any of the insider types of risks that could go on and, in fact, it's the insiders who are affecting all these controls and doing all these audits and, you know, all the secrecy, and trade secrecy of computer software and whatnot, you're not going to achieve any dent in this voter perception that these risks are out there and they haven't been addressed properly.

And so, that's what I consider the task of the VVSG, is that it needs to be completely rewritten to take insider risks into primary concern and address the types of risks that voters are concerned about. I mean it means nothing if we put a stamp on these and say that they're certified, if the voters still believe that they're faulty.

DR. KING:

Okay. Larry, John, and then Mark. Barbara is your tent back up?

DR. SIMONS:

I'm sorry.

DR. KING:

Okay. And I think in the interest of time moving forward, Mark, I'm going to let you have the last word on this question so Larry, John, and Mark.

MR. NORDEN:

And I'll be quick. I just wanted to follow up on something that both Barbara and Rebecca touched upon, which is that, you know, when

it comes to convincing the public that things are fair and restoring trust in elections and in our system, I think, where possible we should be as transparent as possible and we should conduct audits when we can. And, you know, that goes for auditing machines and it goes for, you know, I think a lot of practices in elections when voters are purged from roles. I think it would be beneficial to the public to be able to see the processes that are involved. Not because I think there are a whole bunch of corrupt election officials around purging people illegally from the roles but it's, I think it's helpful for the public to understand what the processes are and to see how they're happening and that they're applied fairly. And, you know, we see audits in other fields, in finance and in business and if we're capable of doing it, I see no reason why we shouldn't do it in elections. Certainly public confidence in elections is extremely important to our democracy.

DR. KING:

Okay, thank you. John?

MR. WASHBURN:

I will be very quick as well. I would say that you're comments on the statewide voter registration systems would be beyond the scope of this meeting since it's on the VVSG. But is there a risk forum for the other elements of our voting system, such as the statewide voter systems? I haven't seen anything like that. And the reason I bring it up is because with the statewide voter registration lists, they have demographic details down to the zip code level, since it has your address.

Well, in my City of Milwaukee or even in my Village of Germantown, depending on how hard I scrub the data in the high transient areas such as around Wisconsin and Milwaukee or Marquette or other high apartment areas or not, can skew that voter list, likely skew it one way or another for a party. I have never seen any discussion on those kinds of risks for things that are extrinsic to the material in the polling location, let's put it that way. But the VVSG handles pretty much stuff that you would encounter inside the voting location.

And as for transparency, I can attest to Mr. Norden's thing. Last September, November, September of 2006, I just wanted to follow the memory card from one polling location to its security. As they left the polling location, I asked where they were going. That's a secret, is what I was told and I have that on video. And I am so glad I did it because I doubt anyone would believe me. Anyway, that particular poll worker has been chastised by the election administrator but nonetheless; my particular little experiment in transparency was thwarted that night. And so, transparency is important but I was just curious if the EAC would consider risk assessments for those areas outside of the VVSG, such as statewide voter registration lists procedures, things like that.

DR. KING:

Okay. Mark.

MR. SKALL:

I also hope to be quick. One of the regrets I think that we have is, when we had the threat workshop at NIST, the goal, at least one of my goals was to essentially be able to track various threats we had

identified and talk about the requirements in the VVSG and specifically the security requirements, as mitigating specific threats, so we have traceability. And Rebecca brought up a point about insider threat. That clearly was one or more than one of the threats that were produced at that workshop and although we never did end up putting in the VVSG, traceability from requirements of threats, that was clearly one of the threats that was considered and many of the security requirements are intended to mitigate those threats as well. So that certainly was considered, although not documented.

DR. KING:

Okay, thank you, Mark. Well thank you. We're making great time and I appreciate all the input on the first question. Matt could we go to the second question?

MR. MASTERSON:

Um-hum.

DR. KING:

How can innovative systems be evaluated for purposes of certification? And how can we create a certification process for innovative systems that isn't a back door around the standard certification processes but at the same time isn't so cost prohibitive and restricted that it in itself becomes a barrier to innovations and newcomers to the industry? And Rebecca has volunteered to introduce this question. Rebecca.

DR. MERCURI:

Thank you. I think, when I was contemplating this particular question, the reason that it came to my mind as the one that I'd like

to talk about, is because I feel that the concept of the voting systems innovation class and also which was the sort of related software independence requirement because both of these sort of play off of each other. I believe and you'll see this in my opening statement, that these are oxymorons. I don't believe that these are actually correct definitions. I think it's a way of providing some framework that really is inappropriate.

And one of the things that I feel about the innovative class is that, essentially if we need to have a special class for new types of voting machines that don't satisfy the VVSG, then what it means is, that the VVSG is inappropriately defined. And one of my pet peeves, with again, this VVSG, as well as, all prior VVSG's is that it's defined in terms of a design requirement. In other words, you know, what the screens are and how many ballots you shove through before you get an error. And these are design requirements and not a functional requirement.

The functions of voting are fairly straightforward and simple. You want to be able to create your ballot. You want to be able to cast your ballot. And you want to be able have that ballot counted the way you cast it and have originally recorded it. And nowhere really, in this 500 and whatever page document of the VVSG, does it really address these functions. There's a lot of, sort of shell around it but it doesn't address these particularly. And so if you have to have a whole innovation class that needs to have a different way of evaluating special new systems that don't fall under the auspices of the VVSG, then what you're really saying is that the job actually hasn't been done correctly by writing the VVSG.

Now let me go on a little bit and read to you from the document of voting systems innovation class that we were sent as part of this. It says -- as part of this discussion. It says right here on the second page, it says since there's no universal measure of security, the TGDC defines the following security requirement relative to existing voting technologies. Now remember, this is within the innovation class. A reasonable case must be made that the new system is, when taken as a whole approximately as secure, transparent, and auditable as existing systems permitted by the 2007 VVSG.

Now many of us believe that these systems that are going to be permitted by the 2007 VVSG, are not secure, transparent, or auditable. So any new system is also not going to be secure, transparent, and auditable. Now this may seem sort of ridiculous but when I read this, I read the follow up sentence and it says in particular, the innovation process is not a back door by which vendors can get systems approved that are less secure than what is approvable through the ordinary process. Oh, okay, since the ordinary process is lax to begin with, we let lax systems through and then we'll let new lax systems through, too. And again, I'm not being facetious here, that's what this says to me when I read this. And what it also says to me is that there -- we know that in the ITA Program there has been some inequities among vendors. Legacy vendors do seem to have sort of almost a fast track because they don't have to get as many things recertified or they can go through quicker. And what this means is, that new innovative systems are going to take a slower time and maybe if they are completely new

they're going to have to take a really, really slow time because we don't understand them. And again, this means to me that this is just depiction of the VVSG being incorrect, that the VVSG itself has been couched into the framework that it doesn't recognize alternative methods of voting and they don't fit into its formula.

Now again, related to this, as I had mentioned earlier, when this innovation class came up there was also this concept of software independence. And software independence is defined by NIST and by Ron Robess [ph] who have written the most on the subject and Ron I should say, read my testimony and wasn't terribly pleased and sent me an email last night. So, but I'm going to go ahead with what I have to say anyway.

The definition of a software independent voting system is, if an undetected change or error in its software cannot cause an undetectable change or error in an election outcome. And so, the question is, can we put this into the innovative system? Can we come up with software independent systems that will affect this particular thing; the change or error in the software cannot cause an undetectable change or error in the outcome? Can we come up with new innovative ways of dealing with this?

And again, the word cryptography and maybe, because Ron Robess is a cryptographer and he's heavily involved in this, I'm not saying he's prejudice to this, but the word cryptography comes in here. And so, they mention in this innovation thing, they mention cryptographic key certification authorities, public electronic bulletin boards, smart witness devices, multiple holders of shared keys, et cetera, et cetera, et cetera.

Now this sounds like an awful lot of software to me. Now how you're going to prove that this software is independent of undetected changes or errors that cannot cause an undetectable change or error in election outcome just boggles my mind. I don't see anyway. You know, like I say, it's an oxymoron. Software independent while you're using software, I don't believe it can be done. Ron and I obviously are going to be debating on this for some time to come. I have disagreed with this concept but have not spoken out publicly about it, but I will be speaking out publicly more, starting obviously, with today.

So what I'm saying is, that if you're going to come up with innovative concepts and they're going to involve software and that software is going to somehow be independent, I mean, what are we doing? And again from the voter standpoint, how does the voter know that the software is independent or that this innovation class actually does the things that, new things, that it says it's supposed to do to make things better? I'm, you know, I'm at a loss to understand how that's actually going to occur. But anyway, that's my comment to kick it off...

DR. KING:

Okay.

DR. MERCURI:

...and you take it from here.

DR. KING:

Thank you, Rebecca. But before I call on Mark and Barbara and then Zinelle, for the benefit of those who may not be as close to the VVSG as some of us, one of the again, outcomes of the current

testing procedures or certification of voting systems, is, it's become a very long process. And estimates now are perhaps a year, year and a half, or two years to test the system. And one of the concerns that's been addressed from both technologists and advocacy groups is, that, if an innovation is needed, if something changes in the mix that requires an innovation to move to the market, given the inertia of the current system, is a method needed to, if you will, fast track innovations into the market? So that's kind of the thought behind it.

I think Rebecca has done a good job of pointing out that the devil is in the details. But that's a little bit of background. And he was first but...

DR. MERCURI:

He's escaped.

DR. KING:

...he has forfeited his status, so I'm going to go to Barbara, Zinelle and then I'll have to sort it out from there. Barbara?

DR. SIMONS:

Okay. I'm afraid I'm going to respectfully disagree with some of the points that my friend, Rebecca made. I actually find the VVSG, the Draft VVSG to be a very impressive step forward, relative to the previous standards that we had and it represents a lot of, I think, very hard and dedicated work. Like anything, it's not perfect but I think it's a very impressive move forward.

DR. KING:

Would you say that again when Mark comes back into the room?

DR. SIMONS:

Oh, sure. I'm speaking for Verified Voting at this point but this is also my view, too. And two components of the VVSG, which I think are critically important, are the notions of software engineering and independent voter verifiable records. Now they may not be -- I mean, I actually find the definition of software independence pretty clear, but maybe that's because I worked at the mathematical and the computer science end and as a mathematician, I find it a very elegant definition.

And, but of course the topic was innovative classes. And we don't want -- it's clear that the new VVSG, the VVSG Draft, has a lot of requirements and these things will take time. So, on the one hand, we don't want to have the barrier so high, that it's impossible for new ideas and new vendors to enter into the field. On the other hand, we don't want to compromise excessively, so that we get bad systems or substandard systems or systems that are not up to the par that we expect of the systems that satisfy the 2007 standards brought in. So there's obviously a tradeoff and it's going to be a delicate thing to do.

We do not feel there should be compromises made, in terms of the standards. On the other hand, given the complexity, the complexities that we're talking about, we think it's very important to emphasize the software independence and the SI and IVVR, because this gives us a way of dealing with these systems, such that if, how could I put it, we don't want to give up important standards but if we have to make shortcuts anywhere, don't make them there. In other words, we need software independence, we need IVVR because this is a way -- this is what we need to be able

to do, audits, statistically significant audits and if we give them up, we won't be able to do these audits.

So, I think these are critically important, so I guess the summary is, the VVSG is a big step forward -- I was told to repeat that when you came into the room. We don't want to make compromises for innovative classes, but we also don't want to give up the software independence in the IVVR because we need that for audits.

DR. KING:

Okay, thank you. Zinelle and then I'm going to come back and get Mark.

MR. OCTOBER:

Okay. I have a couple of thoughts on this. In a lot of ways, I find this related to the first question, actually. I guess before you decide what you'll compromise; you have to think about...

DR. KING:

Move that black flat microphone a little closer to you, thank you.

MR. OCTOBER:

Sure. Before you decide what you compromise, you have to decide what your risk assessment level is, which is what we talked about in the first question. And like Barbara, I guess I get concerned when we start talking compromise. And I guess, we have to focus on what's most important, in terms of, sure it may fast track it, but if we're going to lost some important factors that increase reliability and security, then maybe it's not so worth it. So, I think we kind of have to keep that in mind. And also it goes with the transparency discussion that we had earlier in the first question, as well. I mean,

we still have to be able to increase confidence of the voter that these things are secure. So I think we need to kind of keep that in mind, what can we give up in terms of opportunity cost? Is it worth it? Is it worth it compared to the time that we'd save? Things along those lines.

DR. KING:

Okay, thank you, Zinelle. Mark, and then Lillie, and then John, and then Rob.

MR. SKALL:

The voting standards have had a long history of promulgation of quite a few different standards. Many industries have many, many standards. The problem when you have standards that replace each other every few years is, you have change and you have a mixed target for vendors and for users of that system. So there are only two choices. You could write a standard, discover later that there are new features, new innovative features you'd like to get in, either ignore those or write yet another new standard.

The option of writing a new standard every two or three years is untenable. It doesn't work and it would destroy basically the voting community. So the innovative system was put in for that very reason, to encourage new ideas that you don't want to ignore if they're there. You move them into a standard. You don't want to create a whole new standard, so there's a way to include this as a module in this system. This is not a new idea in standards. Many standards we've been identified with have features similar to this. The part that Rebecca talked about, all it says is, that the intent of this is not to create a whole new yardstick for measuring

conformance. The key to any standard is, requirements and how one does conform to those requirements. All it says is, they have to meet the requirements already in the standard for conformance. That's all that was saying.

So again, this is an attempt to encourage new thoughts when they come up and they may not be appropriate. If they're not appropriate, they won't get voted into the standard, to be put into a standard, without creating a whole new standard and creating chaos.

DR. KING:

Okay, thank you. Lillie and then John.

MS. CONEY:

This area of discussion is looking at the evolution of voting systems. How do we create a dynamic environment, where new systems that are better or provide a higher sense of reliability and accessibility, usability, and so forth, can effectively compete and find its way into the poll place environment, without sacrificing the security of the standards, the goals of standards development?

What we've seen is, that it may not be an entire system. It may be a component part. It may be something that's viewed as being an improvement like electronic poll books. They find themselves inside the polling location and there are no standards of process that led to that technology actually being vetted and used. And it literally is connected to technologies that may have went through the standards making process.

So how do you actually assure yourself that the hard work you did to create these standards and hopefully find ways to make

standards a relevant and effective means of screening bad systems out of the process are not circumvented when you put this new, small component technology into the process and then allow for it to work and literally beta test with voters, during a live election. It's a -- and we've seen this happen. And so, the failures identifying the weakness actually happened during a live election and then they tried to -- the effort is then to modify it and work on the process to make it work better for the next election.

This is a very tricky area. How do you define innovation? How do you define, not an upgrade of software modification and where is that line going to be in and who's going to make the determination? And how do you make that transparent to all of the parties that come to the table and have a vested interest in how an election is actually going to function with technology?

Promoting evolution innovation is very important but the market force is, the cost factors are real. This is not like any other economic model that you can compare it to. Elections are not for the most part, a profitable business enterprise. The margin of value that a company might put into R & D and then expect to get out over the term of the use of the technology, is directly affected by what happens in the standards process, what happens in the courts following elections, what happens when -- with voter's satisfaction or even outcomes of elections, where there are perceived problems can have a long-term impact on all of these decisions that go into the process.

But ultimately, we have to worry about this process for the voter's benefit, making elections very voter centric. So, do we look

at R & D -- this is beyond the scope of the VVSG but some real discussion that has to take place. Should R & D be primarily the responsibility of the federal government, opening up the findings of the research that may be beneficial to the commercial sector to be able to take those developments and create innovation and technology? How do we make sure that there is some kind of level playing field for those new ideas of new innovative products that may actually accomplish a lot of the things that we'd like to see for elections find their way into the stream and have a reasonable shot at actually being considered and adopted?

We have a lot more people at the table thinking about elections, technologists, researchers, academics, policy people, as well as, private actors out there, who may be coming up with ideas and innovations that will be very beneficial but it's a very difficult market to find your way through and find a place at the table.

We have to think about all those things when we think about innovation. I think there are some opportunities but I also think there are some risks. And as Zinelle said, the risk and opportunity, we have to quantify and create a matrix for to measure, so that we understand when we are looking at innovation that we're not sacrificing voter confidence of voters being able to effectively be heard through the process.

DR. KING:

Okay, thank you. John, then Rob, and Larry, I'm going to let you have the last word before break.

MR. WASHBURN:

Well I would like to start out by saying the 2007 draft does represent an incredible amount of work on the part of NIST and it is a significant improvement over the currently enforced standards of the VVSG, 2005 VVSG, and the 2002. I especially appreciate that you took out Appendix B5 because that's currently in the 2002 and 2005 VVSG, which says, no system need conform to any requirement in the standards requirement and that's essentially what Paragraph B5 says. So it was a standard that said you could be exempt from any requirement of the standard. I was -- the reason I put up my tag is, you said that currently the projected time frame for certification, from start to finish, is one year.

DR. KING:

Between one and two years.

MR. WASHBURN:

And that's under the 2005 VVSG?

DR. KING:

Um-hum.

MR. WASHBURN:

I find that astonishing, because the 2005 VVSG is, at best, a minor incremental improvement over the 2002 VVSG. How is it the same personnel doing the review and the testing are now taking a year to two, when they took months before? I mean how did that happen? So I'd be interested to know the answer to that question. But as for the innovation class...

DR. KING:

It's a secret.

MR. WASHBURN:

Yeah, every time I ask a question related to how is this stuff tested, I am told it's a trade secret, hence, the coffee mug, which you can buy any other clothing item that has it as well. But and it is my pet peeve is that, the very asking of the question is considered a trade secret -- or the answer is a trade secret.

But the innovation class, the questions on the innovation class, given that the time frame has moved from months to years and given that the 2007 is such a quantum improvement in the 2005, in terms of specificity and rigor, how is that not going to stretch to five years? And how does that not create the economic incentive to use the innovation class as the way to shorten that two to five year testing framework to something more reasonable, like one or two or six months? I don't see how the economic and -- rational economic incentive doesn't drive you to that.

DR. KING:

Um-hum, thank you. Rob and then Larry.

MR. RICHIE:

I wanted to echo both of -- or second both of those last two comments. I thought there was a lot of interesting points made in the fact that government, potential government responsibility for R & D and just looking at the certification timing process, just to reiterate, you know, again the lens that we look at through is through ranked voting methods often and it's just taking a long time.

So Sequoia had the system that's been in certification for, I'm not sure how long, but the City of Oakland had passed 69 percent to use in instant runoff voting. They didn't get that certified in time and now it's going to have half of it's city council elected in

June, as part of the runoff system, in which turnout will be about 10 percent and if we had been certified on time they would have had an election in November, when turnout would probably be much higher, 80 percent or so. It has real life impact. It's also creating havoc for Pierce County, Washington, a county of 800,000 people which have a big county executive race and they don't know if their system is going to be ready.

MR. WASHBURN:

Ten percent is a better beta test.

MR. RICHIE:

True. The -- issue also sort of attaches to what John and Lillie said, is, that we are of an industry, you know, a trade, to run these elections. And if we had a different kind of system, when you had something like Pierce County, Washington or Oakland wanting to use the rank choice system, you could imagine the software patch, or something, that being added to a system that could be universally applied. Some company would develop a patch or the government would develop a patch with a company and it could be added but of course it can't be added to each, because each system is different and each system is not transparent and that's part of the issue is that each company has to come up with its own way of doing things.

And then added to that is, that each jurisdiction might have little refinements, say, of how you do a rank choice system. And, you know, there's different little variations and what we're finding is that companies feel it's very inflexible. Like they do it one way and then another jurisdiction has a slight difference. They say, well

we'd have to go through the whole certification process again and that would cost hundreds of thousands of dollars and, you know, this jurisdiction which essentially has passed the same system can't -- might not be able to do it unless it, you know, re-passes a charter amendment that makes this very slight change. So that the -- in an innovative class, the points that we wanted to suggest is that if there is a minor change that can be tested easily that that can somehow be fast tracked, and again these little variations of say how do the algorithm of doing a rank choice system.

For the issue of the recommendation that we wanted to point out there that was in the testimony, kind of the main part of the testimony that we've presented, is that if it is highly transparent that the change could be fast tracked, in this sort of innovative class and our definition of that, was proposed to be two things. One, the system has a clear and non-controversial audit method that allows for re-tallying elections, using the original voter inputs, such as hand counting for marks on paper ballots. And that the system uses exclusively commercial off the shelf electronic hardware in either commercial off the shelf or open source software that can be widely and formally tested by outsiders.

And this has come up with, say the State of Vermont, the legislature passed instant runoff voting for congressional elections that they were to use this November. The Governor vetoed the bill that might have come into play this November. And there are ways that that could have been done using -- with that standard that would have made a lot, been a lot easier than what the state probably would have done, which also was reasonable but just a lot

more difficult. And that if it can meet those standards we thought that that could be a way to measure when to fast track.

DR. KING:

Okay, thank you, Rob. And Larry you no longer have the last word, that's going to go to Brian.

MR. NORDEN:

Okay. I just wanted to follow up on a couple of points that Lillie made. One is I agree, I think encouraging the development of the innovative systems is certainly a good thing and something that we would strongly support, as long as we're constantly aware of the potential tradeoffs that are involved. And the second point, that is a little bit more of a lawyerly point, but as Lillie said what, we're defining as innovative class would be helpful. And I think that that's not particularly clear in the VVSG. In my written testimony, I don't know if it works, but I presented what might be a more clear definition of innovative, of an innovative system. And I said a system that performs or supports voting activities and does so in a manner not contemplated by the guidelines. Something like that might be, I think might be useful to have in the VVSG.

DR. KING:

Very good, thank you. Brian you're between us and our break.

MR. HANCOCK:

Well I certainly won't take long but I did want to take post prerogative to have the last word in this one instance. It will probably be the last one. Just to address the issue that you brought up about the certifications, since that's kind of in my wheelhouse here.

Certainly, the two things we know, that certification now is taking longer and it's more expensive than it has been in the past. I don't think it's a big secret though as to why that's happening. You know most of the systems, most the voting systems went through the NASAD process, especially towards -- they were legacy systems, they're modifications testing. They shouldn't have taken as long. We made a very conscious decision at the EAC to not rely on any of the testing that was -- happened in the past. We want everything to start fresh and so every system that we have accepted is essentially starting as a brand new system whether it's been tested in the past or not. So that's starting to take a little bit longer. You know in the future when those systems are EAC certified and there are modifications to those, they're certainly going to have a much more streamlined certification process, but we do want to get it right. We are working with NIST.

You know the process, again is more transparent. I wanted to address that too. We're posting test plans and we will be posting test reports. NIST and the EAC are currently working on test methodologies that we will be requiring the labs to use, that will be public, that will be out there for everyone to look at. You know and so this is sort of an evolutionary process. It's not all happening immediately but I think we're moving in the right direction as far as that's concerned.

DR. KING:

Yeah, well thank you for that clarification.

MR. WASHBURN:

But the same personnel. You and Mr. Wilkey were doing the reviews with NASAD, as to whether the labs were doing anything. Mr. Dearman, Mr. Southwards, Ms. Coggins, they're the same people doing the testing now as was doing it under NASAD. What changed? It sounds like, what it was is, under NASAD, you guys were allowing them to say, we won't do the whole system, in contradiction to NASAD's own public requirements of how to do the testing that when there's a new system with a new component, the new system has testing de novo. And sudden -- and now essentially that's what's taking so long, is that because we are now actually enforcing that de novo requirement?

MR. RICHIE:

Can I say and just throw in a second question is is it a matter of...

DR. KING:

Excuse me.

MR. RICHIE:

Oh, sorry.

DR. KING:

Excuse me.

MR. RICHIE:

Okay.

DR. KING:

The tent and...

MR. RICHIE:

Sorry.

DR. KING:

That's all right. I do think and Rob we'll come back and take this, but I already promised the room a break and people have paced themselves. The restrooms, there's a key on the counter, blue for men...

MR. MASTERSON:

Yes.

DR. KING:

...and pink for ladies. I think that's how it works. Just grab the first key and head to the door to the -- by the water fountains and the restrooms are around the corner. Let's take fifteen minutes and let's be back right at five minutes till the hour and we'll go from there. Thank you very much.

***

[Recess from 10:37 a.m. until 10:56 a.m.]

***

DR. KING:

Okay. We're about to restart. The first thing that I'd like to do is to recognize that Commission Carolyn Hunter has joined us. Commissioner, good morning. And I want to emphasize, first a goal and then a request to our table. We have an hour now left to address four questions and our past history has been, we're well within our comfort zone on that. These are essentially the same six questions that we've asked each of the discussion panel. And one of the important things that this provides the EAC, is the ability to look at these six issues through the lens of all of these different panel groups and what their concerns and what their priorities are.

So it's very important that we get through these questions, so that we can kind of complete our analysis of the responses.

To that end, I want to make sure that we really try to focus our comments on this draft of the VVSG and on these questions to the extent that we can. And remind everybody here, including members of the audience, that the EAC has a website that can be used to solicit comments across broader issues related to the VVSG and, in fact, the EAC's certification program in general. And I encourage each of you to take advantage of that. So, if it's something that we can't get to at the discussion table here today, it certainly doesn't mean that it's not important and it doesn't mean that you shouldn't take advantage of the written input media to do so, thank you for that.

Matt, are we -- is Question 3 up behind me? Question 3 has to do with the methodologies of, I'm sorry, of open-ended vulnerability testing. And that's not a new concept in security but it's certainly new to this version of the VVSG. And I'd like to ask Mark if he would to introduce the topic and put some context to that question.

MR. SKALL:

Thank you, Merle. So for, the first point I'd like to make is, probably in retrospect, if we had to do this again, we wouldn't call it open ended vulnerability testing. And if you think of it really as expert system review, I think that makes more sense and maybe we should have called it that. But what it is is essentially what people call red team testing. It's a team of experts and the way it's defined in the VVSG, there are three security experts and one in election

management, comprising a team, probing a system, primarily looking for security glitches, vulnerabilities, however, if they find other issues, clearly they would report on those as well.

Typically this type of testing is done after conformance testing so you would have a conformance test sweep. You would thoroughly test an implementation of voting system for conformance. Test every single requirement that's in the VVSG and then afterwards you would assemble this team. Now in the VVSG there is no time sequence mandated. We typically think of this being done at the end. One could choose to do it in a different sequence. The VVSG mandates that there must be a minimum of twelve staff weeks devoted to this. And there are -- you know, one of the issues with this type of testing is clearly, subjectivity and we would like to make it as objective as possible.

By the very nature of this type of testing, there is going to be some subjectivity but there are pass/fail requirements in the VVSG. Certainly, if during this testing we find that a requirement has been violated, clearly that's something that one would fail the voting system for. There are other pass/fail requirements that are a little softer, things like, you must show that various threats or vulnerabilities have been appropriately mitigated. And if one finds a vulnerability in this that could change the outcome of an election, can be exploited, that's another reason to fail someone in this type of testing.

So there are many challenges, with one them again, being the subjectivity, the second being the uniformity. Clearly you would like different testing labs that test a standard to always come up

with the same results. And when it comes to conformance testing, one of the things we are doing at NIST is developing a comprehensive public test sweep for this version of the VVSG, to be used by all test labs, which will certainly enhance consistency. However, when it comes to open ended vulnerability testing or expert system testing there are challenges because clearly different teams may come up with different results. One of the things I've thought about in the past is whether, in fact, you could have one team representing all the labs like a representative from each lab, so you have only one team and that would ensure consistency, but clearly ensuring consistency across testing is one of the challenges.

DR. KING:

Okay, thank you, Mark. I'm going to ask Brian to clarify on Question, is it C, up behind me? I'm sorry, yeah, Question C, if the EAC were to require OEVT, how could it be best included into the EAC's testing and certification program? It occurs to me, that it might be constructive to get a little bit of background about the distinction between the standard itself and the program that administers the standard.

MR. HANCOCK:

Right. And I think this falls right into what Mark was saying and really, one of the reasons we're asking this question is, we want to know, you know, where this really fits into the system. You know, Mark, we talked about it being included as part of the standard but there's also, you know, an equal amount of evidence that would suggest it really should be, you know, part of the conformity

assessment system for the voting systems. You know and we've kind of gone back and forth about that. You know, is it -- should the open ended vulnerability testing be very detailed and put in the standards document, you know, or should there be some flexibility. And if the, you know, brought into the conformity assessment system and the EAC be free to adopt policies and procedures with the input of the community, of course, on how to do that? And so, these are questions that we've been sort of going back and forth with for quite some time and the reason that we brought it up to this group here.

DR. KING:

Okay, thank you, Brian. Rebecca, and the John, and then Barbara.

DR. MERCURI:

One of my pet peeves with the -- this VVSG or my many pet peeves with this VVSG, as well as, the earlier ones, is that there is no methodology for decertification. And one of the problems with not having decertification is, that if you truly have open ended testing, in other words, ongoing, in the true sense, not just, you know, a twelve week type of period, but we're saying ongoing testing and if things are being tested out in the field, when we find that there are problems, there should be a methodology to have a recall. If we find that there was a problem that actually should require, that would not have allowed the certification in the first place, we should have a recall of that product and there should be decertification, until that is remedied. Now how that would work again would have to be mitigated by the EAC.

But I'm from the great State of New Jersey and if any of you have been following some of the post Super Tuesday things that have been going on in New Jersey, we've had some problems with the Sequoia brand voting machines that we have there. And a number of Princeton computer science professors had offered for free, to test these machines to see what the problem actually was because they were not in agreement with what Sequoia had said the reason was. And Sequoia slapped down a trade secrecy, saying that it would be a violation of contracts and trade secrecy to actually examine these voting machines, which were not counting properly. It's a critical issue and, you know, then this had to be litigated in court. Sequoia, at the time of my, you know, I'm sorry I have to bring up their name but that is the product that we're dealing with in New Jersey. Sequoia hid behind the federal certification and even on their website said, that well, we're federally certified, so it should be okay. Well it's not okay.

And what we're seeing and what I've seen for many years, as I've followed this for many years, is that the certification is being used as an excuse not to fix because I hear from vendors often times, we can't fix this flaw because if we change the code, we'll lose certification. Yes, that is true and, in fact, you should lose certification. You should lose it before you change the code because if you need to change the code, you need, actually to be certified -- decertified.

And that's what I see as the value, as the question asked, of the open-ended vulnerability testing model. It should be an ongoing process and there should be a process of decertification in

addition to, you know, in sort of companion with the certification process. There needs to be a way of eliminating products that are just not making the standards correct, if they're not meeting the standards.

DR. KING:

Okay, thank you. Then I've got John, then Barbara.

MR. WASHBURN:

Well, there currently is a process under the 2005 VVSG for decertification but it's in a separate technical document, called the Voting System Testing and Certification Program Manual and that gets to one of my problems with the VVSG, the testing program manual and the National Voluntary Lab Accreditation Program, also known as NVLAB, that NIST sponsors, is that these three elements of the framework are done in isolation. They seem to be done in isolation from each other without a real consideration of the impact a change in one has on the other or how can they be altered to harmonize better to achieve what we hope is an outcome, that as soon as the defect is discovered it can be thrown into the decertification process under the program manual.

But I think some of the issues with the program manual, is the EAC missed a golden opportunity to make a requirement of the manufacturing registration process that you don't have trade secret. Right now unfortunately if you wanted to assert -- if you wanted to do an examination required, you run across a takings clause of the constitution. Had that been included before the first vendor had submitted under the manufacturing registration that would have been moot because they had given up the trade secret protection.

So to some extent, that was a missed opportunity that I don't think we can go back and fix.

The -- as for the red team testing, I believe the EAC has the authority right now to do it, under Section 241 of HAVA, specifically Paragraph 19. So if you want to sponsor the University of Connecticut, who's doing great work with optical scanners, or Princeton, or Berkeley, or MIT, go right ahead. You can do it right now.

But my question is, what do you do with security defects that are ruled to be in conformance with the spec? And this is not a moot question because the security defect with the interpreted code that's on the Diebold TSX and touch screen and the optical scanner both the AccuVote models, as well as, the fact that the ESNS scanners have a complied, a freshly compiled EXE that gets run and it's distinct and unique for each election jurisdiction and ballot style. I mean, they compile a fresh program for every election jurisdiction. Well, those have been ruled, as in conformance with the 2002 spec.

So, I guess one of my questions is, okay, you do your red team analysis, you find a defect, but it doesn't strictly violate the standard or if the -- through the appeal process that's found in the program manual it's discovered or it's ruled it's not, what do you do with that kind of defect? So, we haven't asked questions of, what do you do with the outcomes of what you do discover through the vulnerability testing? And that's it.

DR. KING:

Okay, thank you. Barbara, then Lillie, then Mark.

DR. SIMONS:

All right so, again I think that, including the red team testing is a big step forward in the VVSG. One of the problems that a number of us had with the previous standards was that, there was a list of requirements and there's no way you can adequately test software by just having a checklist. It's just not possible. So, I do think this is again, another step forward. There are -- and I also think that, if a voting system fails multiple times with this red team testing, that should really raise a red flag, if you will, as to the quality of the product that's being tested because that shouldn't be happening.

On the other hand, again, this is another one of these areas where we're encountering tradeoffs. The testing is going to be only as good as the testers. And as John said, the EAC could, right now go out and get University of Connecticut, or Princeton, or MIT, or Berkeley, or a number of other places to -- maybe not the right number but...

MR. WASHBURN:

Who are, really, largely doing it for free?

DR. SIMONS:

Right, who are doing it for free but actually I think you named almost all of them. And a number of these, I mean, I know, for example that some of the people who have been doing this testing don't want to keep on doing it because they are academics and they don't get credit for doing it. They're doing this as a civic duty. And we've been fortunate for example in the California top to bottom review, to have University of California led teams, which are really, with cream of the cream, in terms of, well, I mean, obviously

they didn't have everybody, but they had some very good people doing this testing and you just can't expect to maintain that standard. You can't have some of the top names in the country doing this all the time, especially when this is not actually part of their job descriptions. So the testing is only going to be as good as the testers. So that's sort of the on the other hand, part of the testing. And I don't know how you address that. I suppose we need standards for the testers too but then, you know, it gets a bit circuitous.

Another -- a suggestion that we have is, that EAC officials and perhaps state election officials should be able to order these tests any time they think they're necessary. So if they see a problem in the field, they should be able to say, okay, this software, this machine gets pulled out and we're going to do red team testing on it. But again, I mean, there's a twelve staff week requirement in the VVSG. Now I don't know what that means exactly and one question I have is, does that include for example clerical support? Does that include the time taken to learn how to use the system? The time taken to write up the results afterwards and what happens, if at the end of the twelve weeks they come across something which looks like it might be egregious but don't have time to pursue it?

So those are again more questions. I don't know how one addresses it because if you allow totally open ended, then it could be a never-ending process and then things don't get certified and the cost becomes astronomical. So I find myself, we find ourselves finally going back to, yet again, the need for being able to audit

systems because we can't do these things perfectly and we can't continue testing forever. So we need to have the option to be able to audit, which means software independence and IVVR and required audits.

DR. KING:

Okay, thank you, Barbara. Lillie and then Mark.

MS. CONEY:

There are a couple of issues with this. There are the way the private sector functions, how you create something that's original, innovative, you get a trademark, you get a patent and it's yours. And you don't write it on billboards and you don't publish and you don't make it available, in details, of how the technology works, available to the public in general or to experts at conferences and so forth, especially if it's going to be negative. You're not going to say hey, you know, this is the worst way you could possibly do DRM or something like that. There's a tendency to keep the dirty laundry inside and not let it out. And we've seen this progression of bringing in elections officials into that world, that we don't talk about what's bad outside of our friends and family, very close friends and family.

But the way innovation happens in the world of technologists and researchers, that's the goal. You find something that's interesting and unique, you figure out how to break it, and then you talk about how you would address those issues of vulnerability or insecurity and make it better and you publish. You write about it. You get credit for it. And if you come up with something that's truly innovative and unique, then you will be recognized as someone

who's discovered that particular thing. That goes counter to how the world of election technology and innovation has taken place.

I think that downstream testing, we were talking about at the very beginning of the process, test, test, test, and try to get it right and then deploy it and when you find it in polling locations then it should be as it should be. But the closer to the voter the testing can take place, the more accessible to testing, red hat testing, for elections officials and affordable for elections officials to do this, I think it will serve the election process to a great degree and inform that process.

The people who are going to be more available to elections officials, are going to probably be researchers at local colleges and universities. So being able to set up the matrix for testing, that it's apples to apples and it's the definitions and the research that comes from that would, actually match up with what's going on at the federal level, so the language is the same language, the terminology is the same terminology, the matrix and the measures are the same matrix and measures. Because we know testing and testing facilities are not equal, so you have to make sure they are as close as possible, so when they're both speaking to the technology and speaking of the technology, we can have a reliability in the fact that we're reading something from this testing facility that's a federally certified facility and we're reading this about what was done in a local test done by -- conducted with an elections official, that we can have some confidence in what we're reading.

But we also are going to have to deal with the fact that elections officials are being asked to sign onto these agreements through the policy environment of corporations that have a vested bottom line interest and not letting others have access to the technology in those localities and being able to have what they need from the process with the ability to publish and write about their findings. Those tensions are going to have to be addressed. I think that for the interest of the voter and election integrity, we really do want to have testing downstream, as close to the voter experience as possible, to better inform the process and then a reporting requirement going back up to the testing and certification process. We would take those tests into consideration and truly consider decertification of systems that aren't -- that show that the system that was tested is not the system that's being deployed as it relates to the software, the hardware, that was put through the testing process. That there are some serious consequences if that is found to be the case, which helps to create self policing by the industry that are actually selling this technology.

DR. KING:

Okay, thank you, Lillie. Mark?

MR. SKALL:

Thank you. I just would like to address a couple of comments I heard, first by Rebecca that the VVSG doesn't account for decertification. The VVSG not only doesn't account for decertification, it doesn't account for certification. Certification is not within the scope of the VVSG and I just wanted to make sure, because it's not clear to me everyone understand the distinction.

There's usually, this chart I show, because I'm a standards geek at heart, which shows the standard at the bottom, tests next, policies and procedures, and then certification. And in many different arenas you can stop at any level. Many areas just have standards, nothing else. Some have standards of tests, others have standards tests and certification. They are distinct processes. Now they are related clearly because one depends on the other but it's not within the scope of the VVSG to talk at all about certification.

The question you asked, I thought was a very good question as well. So say during this red team testing you find security defects but they don't violate any of the requirements. There are really two ways to address that. Number one, theoretically, you can still fail them because as I mentioned, one of the pass/fail requirements, is that a requirement has been violated or that a vulnerability found could change the outcome of an election. So if you find that you can fail and even though it meets all the specific requirements. The second real answer to that is in the long run and even in the short run. You change the VVSG, you update it, and you make sure you have a requirement in there that, in fact, makes sure that particular vulnerability cannot be exploited. The bottom line is, you want -- you do find out when you write tests, when you do testing, you do find out many times the requirements are not complete. And there's a feedback loop where you actually can change it so there are two ways to go about doing that.

MR. WASHBURN:

I'm sorry. Part of the feedback loop is that program manual...

DR. KING:

John?

MR. WASHBURN:

I'm sorry.

DR. KING:

Put that tent up, buddy. Go ahead.

MR. WASHBURN:

I thought I was stepping on Lillie's time there. Part of that feedback loop though is the testing manual, testing program manual and it doesn't address those like non-conformance issues as well as that statement you just had, so that's why I was arguing that there's the distinct possibility that you could have a security breach with -- that could be ruled in conformance. And so, as you go through that, as you go up the ladder, the testing has found something but because of the certification or policies and procedures it still gets through, so.

DR. KING:

Thank you. I'd like to make one observation and then we'll move onto the next question if there's no more. And I think John brought up a very interesting aspect of the entire federal certification, how it interlocks with state certification and how it interlocks with state law, state election board rules, and secretary of state rules and regs, customer procedures, all of the downstream implementation issues. And I've often characterized the OEVT issue, like the dog who chases the car and never really thinking through what happens if you catch it. And I think the issue, at the jurisdiction level, and certainly tomorrow when we meet with the county election officials, I'm looking forward to their perspective on it is, what do you do

then? And so it illustrates, I think John's observation, illustrates and Lillie's too, the importance of understanding the VVSG in the context of the program administration and the context of the jurisdiction requirement, to use federally certified systems, and then the ultimate responsibility at the jurisdiction level, to implement elections according to an election calendar. John?

MR. WASHBURN:

Talking about the downstream, in particular with the County of Waukesha, which is the second most populous county in the State of Wisconsin, one of the issues I brought up with a particular system called Winidias (ph), with the county clerk, was that since the software calls stored procedures by reference of name only and since you have the full implementation of the enterprise manager, you can alter the contents of those stored procedures and therefore alter the behavior of the election. And I was having trouble with the technical aspects of trying to explain how this would work and I offered to say, well I can show you if you would like, at which point, as Ms. Coney pointed out, she says, I can't do that because that would be, well aside from her normal reticence of doing that, she said, even if I wanted to, I couldn't. So there is that blockage.

And essentially the reason I wanted to point that out is, because I was trying to make the argument, that the enterprise manager forms a compiler that meets the definition of compiler, under 2005 and 2002 VVSG and therefore the presence of the source code and the sequel statements and the compiler violates a specific requirement and so I just wanted to demonstrate to her that this would be the case. And again, I would have had no problems

going to the EW or Madison, Milwaukee but her point was, is that first off, I'm not keen in helping with that, but two, even if I wanted to, I can't. She would lose, you know, she would be violating, essentially, her non-disclosure agreements and her trade secret requirements with Sequoia.

So there is a definite downstream interlocking there, with -- even if the election official is desirous to do such testing, there are serious impediments, both for talent to do it and setting up the environment and under which it can be done.

DR. KING:

Okay, thank you. Well I'd like to move onto Question 4. We've got about 35 minutes before lunch and I think we'll be right on schedule. Matt, do we have Question 4 up behind me? The question is, do methodologies exist to test voting system software so it can be reliably demonstrated to operate correctly? And if testing to a thorough set of standards is not enough to demonstrate, what else can be done to improve the confidence in electronic voting systems?

Testing methodologies, typically, seek to prove the existence or the absence of features, functionality of systems, and to what extent the attributes of the system achieve the goals of the system. Some methodologies, as Rebecca pointed out, use theoretical proofs. Some methodologies use simulation, others use test-driving and real life situations, that are all -- and then there's hybrid combinations of those.

So, in this question, I think what we're seeking to find out is, can voting systems be tested? That is kind of an overarching

question. And then, if the standards that are being proposed in the VVSG are inadequate or inappropriate, what can be done to strengthen the testing methodologies to ultimately enhance and, again, I thank Rebecca for bringing this up. This is about the voter's perspective, the voter's confidence in these systems. So Larry, I'll start with you.

MR. NORDEN:

Well, I think in answer to the first question, I think my understanding anyway, is, there is general agreement, you're never, no matter how many tests you do and how many different methods you use, you're never going to get the point where you can know with 100 percent confidence that software is going to operate correctly. I would say, certainly adding open-ended vulnerability testing to the process is a big improvement. And in general, I would echo what Barbara said earlier, you know, that the latest or the latest draft of the VVSG, to me is a huge improvement over what existed before. It's a really -- it's not a perfect document but I think it's a great document and it's obvious that a lot of work went into it.

In terms of, you know, what can be done from the perspective of the voter to have greater confidence, that systems are operating effectively and correctly, some of the things, I think the most important things have already been mentioned. Making sure that we're conducting regular post election audits on software independent voter verified records, I think, would go a huge way towards, if it's done transparently, where the public can observe it and has confidence that the process was a good one can go a

huge way towards increasing public confidence that these systems are operating correctly.

Something else that's also been touched upon, is the idea of introducing this closed feedback loop into the process, so that when there are problems, either machines are certified, that there's some way in the regulatory process to deal with that, just as you would have, if an airplane crashed, we would look into why the airplane crashed and we would take steps to make sure that it doesn't happen again. We should make sure that we're doing the same thing with voting systems. Again, I think if the public sees that happen, there will be greater confidence that not only that the system is going to work but that the system is in place to correct the problems when they occur.

Something that I don't know that the EAC has the power to do, now, but I would certainly like to see it happen is, I would like to see the process changed for how testing labs are picked and paid for. I would really like to end this kind of, what I think a lot of people see as a conflict of interest, where the testing lab gets to select -- the vendor gets to select the testing lab and pays the testing lab directly. There -- that's creates an obvious, assumingly appearance of conflict of interest for the testing labs, to make sure that systems pass and I'd really like to see that changed.

So those are a few things I think could increase public confidence that our systems are working correctly.

DR. KING:

Okay. Mark and then John.

MR. SKALL:

So the answer to this question, like anything else, really depends on the definition of words. So the definition of the adverb, reliably, is really the key here. Like everyone around this panel knows, you can only show the presence of errors. You can only prove that errors exist. You can never prove that they don't exist. So if reliably means, to 100 percent certainty, no, the answer is not, but by increasing testing, we try to increase our level of confidence. And the more thorough our test sweeps, the more our level of confidence that we've caught all the bugs. We can never be sure and we can actually be pretty sure we haven't caught all of them but you, at least, can be sure that you've caught many of them and the more thorough you are, the more you do. Again, open-ended vulnerability testing helps improve this.

But the real key to this is this whole concept is what drove the idea of software independence. The whole idea, that no matter how thoroughly you test, that you can never be sure the software works correctly and thus cannot rely on that software working correctly, is what drove software independence, so you have a backup, so you have a way of auditing the systems. And that's the VVSG's answer to that question.

DR. KING:

Okay, thank you. John and then Rebecca.

MR. WASHBURN:

I was going to say one -- the fifth rule in my five rules to testing your voting system is, go where the evidence leads you. And that kind of touched some of what Mr. Norden said, that there's not a real good feedback mechanism that, okay, we've discovered something.

How do I report it and to whom? How does it get followed up on? And just the very fact that it -- that you can watch that process happen, would go a long way to helping assure voters that yes, the process, while it maybe not perfect today, is improving at least, you know, so that it, you know, being the math geek I am, it's asymptotically approaching, you know, a high reliability.

But, and I bring this up because I, in my written testimony, I mention Germantown District I, where the ballot scanner sucked in eleven ballots and apparently never registered any vote. And the election officials discovered this and even though we have a specific state statute that says, if a voting machine makes a clear and apparent error, you're not to rely on its paperwork that prints. The -- my election board, at the state level, basically said, no, that's not for a citizen to report. It's not a criminal violation, so you can't report it to the DA or the Attorney General. It's only for a candidate to bring up in a recount situation, to try to pierce the presumptive correctness of those paper reports.

Well, I've got to admit, that made me very uncomfortable, that, here is a clear documented defect on this particular scanner type, that the answer was -- and it just went right under the dark water without even a ripple, you know, just bloop. And there's millions of people voting on that particular type of scanner, across the country, yet they are unaware, until the Premier put out a product advisory in Florida that, oh, yeah, two years later, that oh, yeah, this happens.

So I guess the -- you're asking if it's not enough, which as Mr. Skall pointed out, 100 percent is not achievable. What else can

be done to improve? It's that feedback loop, a transparent one where you can see that, as things are discovered, the evidence is followed, wherever it may lead, no matter how uncomfortable and dirty the laundry is.

DR. KING:

Okay, thank you, John. Rebecca, and then Barbara, then Lillie.

DR. MERCURI:

Since Larry brought up aviation, I think it's a perfect example. One of the reasons why people have confidence in flying in airplanes is because they don't crash that often. And they do, when they do crash as he said, you know, they go out and check this out and they, you know, they're right on top of it. And when we look at what we're doing with the VVSG and the certification that should not be the goal. The goal really should be voter confidence. The goal should be to establish voter confidence, by having systems that don't do like they did on Tuesday in Pennsylvania and crashing. And, you know, they don't do like they did in Florida, in the contested election where, you know, thousands of votes are missing. That's not going to establish voter confidence, no manner of how much we're going to do this testing and how strong the imprimatur is of the EAC that we put on this, once the testing has been satisfied. That's not going to salvage voter confidence, though I think we need to look at it again from the voter standpoint.

Now getting back to the mathematics of the situation, I brought with me two articles and I'll have them available at the break. One is called Bolics [ph] Ballots and it describes in very plain English. some of the mathematics problems that we have in

trying to do this testing. One of the problems that we really have is. that every election the voting machines may stay the same but the ballot changes every single time. And now there are, you know, maybe one of these innovative systems, there are ways to make sure that the ballot doesn't actually change every time but the way that we do them now is that the ballot is different for every single election and so the testing that we see is not to the ballot faces that's done sort of locally, but it's done to the systems that, you know, put up these ballot faces. And again; that's inadequate. So, you know, we've sort of separated that preparation process out and that's where we see butterfly ballots and other layouts and designs that we're, you know, should have been prevented by HAVA but, in fact, aren't. And you can have a butterfly ballot on a touch screen as easily as you had it with hanging chad. So these are the types of things that are problems.

And then the third one, I brought another article that I wrote, which was called uncommon criteria, although the common criteria is great some -- one of the things that I revealed about it in some of my work with it, was that there are some inherent conflicts in the criteria, as there are in voting systems themselves. There is an inherent conflict between full anononimity and full auditability. Often times people ask me, why can't we vote on the Internet? I vote my stock, you know, shares on the Internet and everything seems to be fine. And the reason why those are fine, maybe they're not totally fine, but they're better than if we did it for regular elections, for public elections, is because those are all traced to me and my shares. Those are not anonymous ballots. So they could

come back to me and say, you now, you voted those 20,000 shares and you voted in this way, was that really correct? And you could say, yes or no. So there is some full auditability and, in fact, that has actually been done in elections, in elections with stocks where there have been questions raised.

So, what I think, what we're trying to say is, you know, you could have methodologies to test these voting systems but you can never avoid the unavoidable, which is these inherent conflicts between anononimity and auditability and testability. So, there's no way to escape from those things, so again, it gets back to trying to establish voter confidence and using that as the goal. That should be the goal, not satisfying the VVSG, but establishing voter confidence.

DR. KING:

Okay, thank you. Barbara, and then Lillie, and then I'm going to let Brian have the final word on this question.

DR. SIMONS:

Well I basically wanted to support what Mark said. In fact, one could show mathematically if you state the problem correctly, that it's impossible to ever know that all of the soft -- all of the bugs are gone from the software but that's a mathematical impossibility. Given that, software independence and independent voter verifiable records, combined with audits, are the only thing we really know we can do to check to make sure that the election results were correct, because we just can't count on the software. We simply -- no matter how much testing we do.

DR. KING:

Okay, thank you. Lillie?

MS. CONEY:

If I may second -- and thank you Mark for mentioning software independence, because I was going to speak to that, as well. Voter confidence is, believe me elections officials understand, the importance of voter confidence in the election and election process because they hear it when people don't feel confident that the election came out as recorded. And so, there is a great deal of sensitivity about voter confidence. What kind of got mingled in to what it means to establish it, keep it high, and not have problems, is not to disclose if there was a problem. There's a great wall of, we don't want to tell people bad news because the reaction will be a decline in voter confidence and being on the front line of receiving the communication from people when there's an effect or an impact on voter confidence, can be very unpleasant. I really am glad to hear that the elections officials will be here tomorrow because they can well inform the process on that.

But, in order for us to really get to the root of problems with voting systems and to really figure out how to create innovation and evolution with technology, we really need to have transparency. We've got to understand what's going on. And part of that, is data collection, creating a matrix for data collection as the root of foundation of auditing as bringing in data to be able to analyze and then report on. And there are a lot of different sources for data, a lot of different types of data that's collected.

The EAC is in a position, not only to be facilitator, but also a domestic diplomatic service around elections, which you well are

aware of all the conflicting interests that come into play and a need to be a calming influence, but also a collaborator and a cheerleader around elections and not an enforcer. Not at this degree. Not the way HAVA is currently written.

But in order to do all of that, looking at the varying streams of data and information that's collected, one is the election protection services that are provided by civil rights groups, election, and voting rights advocates. They've gone high tech and they do a lot of data collection around elections that may be beneficial in trying to understand some of the problems or some of the areas of concern or interests and being -- making room for that data to come into the process and of course couched and described what this information is and how it's being -- how you should inform the process as well as encouraging others to bring information into the system to help inform the evolution of standards development now at a completely federal process, which is very new and it required literally step by step creation of this process, at the same time of doing the standards, at the same time of certifying systems to a standard which had made the process a lot longer than maybe it will be.

But data collection, I think, is key. We've got to be willing to do that. And it's also another means of linking in groups that traditionally would not have been considered in the administration of the elections process.

DR. KING:

Okay, thank you. I'm going to let Brian have the word on this. We've got two more questions we need to move onto. Brian?

MR. HANCOCK:

Thanks, Merle. And I just wanted to just reiterate the importance that John expressed and Lillie and a few others about the importance of the feedback a little bit. In fact, we're -- we've begun that process in our certification manual. There is a requirement that manufacturers inform the EAC of problems with certified, with EAC certified systems in the election. There's also a mechanism, whereby election officials can report detailed, can provide a very detailed report of problems to us.

In addition to that, we certainly have the ability of looking at the excellent information provided by groups out there, like Voters Unite and others, to verify what we're getting. If we don't -- if we see a lot of problems that you're showing on your website and we haven't received any information from manufacturers, that's something we're going to be very interested in and go check that out.

DR. KING:

Okay, thank you, Brian. Question #5, Matt, please. And Lillie had volunteered to introduce this question dealing with the balance between usability and accessibility, security, and other requirements of the system.

MS. CONEY:

I found this question -- one, it's one area of the VVSG Draft, that's very key to the work that we do at EPIC. It's not just usability and accessibility, but it's also looking at the issue of privacy. But for security experts, the notion of -- especially in an election environment, as opposed to other areas where security is discussed or discussed, the issue of usability, accessibility, and

having a secure system, they're competing interests for that. The traditional discussions about security are access but access is usually in the form of limiting access or restricting access. But in the context of elections, we're talking about anyone eighteen years of age or older being provided access to a process that should be very open but while at the same time having discussions around security and then usability.

The one -- the focus is about -- for voters but also in this environment we have to consider poll workers because they are, in fact, representative of the voting population that will be served. And having a focus on usability, we've seen problems with usability, with ballot design, voter interface, where the rubber meets the road, if you will. Problems from paper voting systems from Florida 2000, where usability issues created a hurdle or hurdles that were insurmountable for voters to be able to participate in the process. We've also seen it in electronic interfaces for voting and DRE Systems where usability has merged as being the key factor that resulted in voters not having the opportunity to cast a vote in a particular election for the 13th District, Congressional District because it's one major example that literally took years to try to resolve.

So, the voice of usability and the discussion process, not just at the top of the standards of development, but literally to the design and implementation of ballots on the local level has got to be fully integrated and brought into play, along with the very valuable asset of the accessibility. And there's a nexus between the accessible discussion and the usability discussion because for

the first time you create another opportunity for a huge block of Americans to be able to come into the election process and participate as equals, in a process that is inherently about creating an equal opportunity for people to have a voice in the selection of our leaders in our democracy, making very basic decisions about how resources, tax money, or commitments for the communities for a wide range of issues are brought to bear.

Electronic interface, in the form of DRE's, were an evolutionary step forward, a very important step forward for person who have disabilities, persons who come from language minority communities. It's not -- and it is about the spirit and nature of our democracy, to actually open the door wider and wider. The process was very restrictive and it's something that we should always acknowledge about the future of our democracy. We've had to make great strides in opening that door wider and wider, to allow more and more of our citizens to come into the process to be heard to be -- to have that experience of self governance. And we still are struggling with that today, whether it's local issues, or state issues, or national issues, access, usability, have always been key components of the discussion.

The good things that have been accomplished because we are now expanding that opportunity to others, because of technological advancement, can't be taken into consideration in vacuum. We literally are trying to catch up in voting system and the elections experience. From basically in 2000, it was the 18th Century experience, to trying to bring it into the 21st Century in a matter of eight years. And literally, being able to benchmark and

measure where we are in the process of doing that, without giving up the important value of elections, one person, one vote, that the intent of the voter is accurately reflected. That we try to minimize those incidents where voters are not able to participate in the process or if they are, finally make it into the voting compartment or in front of the voting machine that their will is accurately reflected by the process while still preserving privacy in the form of ballot secrecy and voter privacy.

There's a lot of work that needs to be done. And it's important to have these discussions and maybe we are also going to have to have the discussion, is the technology right to do all these things in tandem? Do we not acknowledge that we have to continue to do R & D in order to get us to that optimal situation that we'd like to be in, with elections? Do we -- does that mean we have to take away something that's been extended to someone else, in order to achieve that? Or do we have a mix of technologies or opportunities to cast ballots where there's early voting vote centers, options for voting remotely or whatever the opportunities may be presented? And if you start talking about that, how does that affect the security aspect of elections, the ultimate goal of elections? And we can't negate any of these discussions. They all have to happen under the same tent and these competing interests are very representative of how the election process works. There's a lot of competing interest that press against each other and hopefully the outcome will be a better process and a system than the one we inherent.

DR. KING:

Okay, thank you. I think that the competing interest is really striking to the heart of this question, which is, in the current draft of the VVSG, there are standards that compete with each other and the most commonly sided one is, security versus accessibility. And I think what the EAC is looking for is, input from the discussion panels on how to go about resolving that. And in particularly in the context of a theme that we've heard at this table today, which is, we can't achieve 100 percent, but we have to make judicious decisions about our priorities. And so, with that, I'll open it up briefly on this question, to any input from the panel. I've got Zinelle, and then Barbara, and then Rob, and Rebecca.

MR. OCTOBER:

So I guess, what I'm thinking here is, we know that the computers aren't perfect. We're not -- we're never going to reach the 100 percent, as you mentioned. But I guess I like to focus on what -- the things that we can control and that we can manage. I think that those are really important and to me usability is one of them. The ballot designs, how does it look? How do people interface with it? I mean, that's something that's purely controllable, at least, in my view and part of getting there so that it's completely usable is involving others, involving advocacy groups on, advocacy groups rather, on how usable something is, how does it look? Do you think this would work? And we have some evidence from that through research as well. But, I think it's something that we can achieve relatively easily and so why not make it as perfect as we can. I mean, continue with, excuse me, the testing to reach the security and reliability issues and certainly accessibility as well, from a

language perspective that's very important, of course, but we want to also be able that -- to be assured that people can interface with the systems fairly easily and they won't have any issues from that perspective. Why not fix that as well?

DR. KING:

Okay, thank you. Barbara, then Rob, and Rebecca you'll get the last word but we do need to keep moving so.

DR. SIMONS:

I, actually, was a bit uncomfortable with this question because I really don't like setting security off against usability and accessibility. Ideally, we should not be doing that. And, in fact, I would just venture that, if a well designed system integrates with -- a well designed voting system should integrate usability and accessibility and security into the system from the very beginning of the design process. Just to give you a quick example, I was told this by a usability expert, a colleague of mine, that when the Mac was first designed, they had usability experts working every stage of the design, because they wanted to make that very usable. And when Apple came out with it, it was heads and shoulders above the PC in terms of usability. It really showed that they put the time and effort into it. So, I think we are facing these problems, in part because; these systems were not designed with these requirements from the ground up.

And I think that perhaps, one of the issues is, rather than phrasing this as a tradeoff between these, what we want to do is, we want to make sure that we don't have unrealistic requirements. I mean we were talking about that before. We can't make the

software perfect. To claim that the software had to be perfect would be an unrealistic requirement. It's not doable.

But similarly with accessibility, there could be unrealistic requirements and I'd like to just quote briefly from Noel Runyan and I know he's already testified before this group, Noel is a blind accessibility expert but I think his testimony is really critical and I would just like to briefly read it, read a very small portion of it. As currently worded, the measures required in the Draft VVSG for assuring that voters with disabilities can have personal independence and privacy in their verification of paper vote records takes several quantum leaps in technology development. The Draft VVSG goes unreasonably far overboard in apparently requiring that paper record verification for voters with disability and alternative language needs, must carry out advanced OCR upon risk ballot parsing and formatic extraction and translation of language other than English. This seemingly desirable super verification system for voters with disabilities would require software and therefore not be software independent. Writing a requirement like this into the VVSG is somewhat like requiring a similarly desirable goal of converting all of our energy generation to diffusion power plants within four years.

And so, I think we need to keep the goals in mind. We want to have accessible systems. We want to have usable systems. We want to have systems that are fairly for language minorities but we don't want to put in requirements that can't be met. Let's not talk about tradeoffs. This isn't a tradeoff issue. This is an issue of putting in reasonable, doable requirements.

DR. KING:

Okay, thank you, Barbara. Rob and then Rebecca and if we can, about one minute each, please.

MR. RICHIE:

I just wanted to first echo what Zinelle said. I thought it was very important and that the issues of pre-election transparency and post election accountability should be built into all of our voting processes. But with the particularly with the usability standards and again, through the lens of our work on rank voting, is that, for example, San Francisco was doing this, there was not public involvement with the ballot design but they received certification on decisions they had made relating to that and unfortunately some people got involved and they changed it but they were going to certify something that really hadn't been tested for usability, as well as, it should have been so somehow that needs to be built in early.

I also think that just as a political point that, if there's a resource connection to this ever, the public does believe strongly in our electoral process and democracy and I think that the EAC and others, it's incumbent on them to communicate whenever there seems to be a resource connection, financial investment connection to a tradeoff and if it could be done with more money, I bet the public would be with us, but we'd just have to find a process of saying look, we're in a position of doing a tradeoff if we don't get more money for this.

DR. KING:

Okay, thank you. And Rebecca, last word.

DR. MERCURI:

There's a couple of suppositions that the VVSG and election administrators and the vendors make when it comes to accessibility and one of them is, one size fits all. The voting machine has to be everything for everybody and it has to work for all accessibilities, a variety of different accessibilities and that all impacts on security because every different type of thing that you add is going create more security problems. And that's not the way that disabilities are handled. You have a certain type of disability; you get a certain type of accommodation device. And so by eliminating this concept of one size fits all that may solve some of these security problems.

The second one, is that we're spending billions of dollars on this accessibility and yes, it's a good thing, but for precinct voting and what about the absentee voting? Many, many, many people, maybe the majority of people with disabilities can't get to the polls. And despite what the HAVA Law says about the polls being accessible, again, I was in Philadelphia on Tuesday. I can tell you there were stairs and people in wheelchairs had to be carried down the chairs. That's just an embarrassment. And so you can spend as much money as you want on, you know the very best accessible voting system but if people can't get there or if they feel embarrassed to get there and if they can't have an accessible voting system as an absentee voter, then you've done nothing for accessibility.

DR. KING:

Okay, thank you. The last question, Matt. Question #6 deals with specific, emphasizing, specific suggestions for altering the scope and the depth of the VVSG in order to improve the cost, time, and

effort required to move a system through, without compromising integrity. And emphasizing that the VVSG itself, is just a vehicle to guide, design, and manufacture systems and one of the unintended consequences that we always look for when we make changes is, how will this impact the implementation? How will this alter the affordability of systems in jurisdictions, knowing that ultimately regardless of who pays the labs, who pays the vendors, it all rolls down to the jurisdictions of voters, in the end to pay for the systems in one way or another.

So putting out the question of, what are specific changes that you would recommend that the EAC and NIST look at in the current draft of the VVSG that would significantly reduce costs of compliance without adversely affecting the integrity of the VVSG? Rob, and then Rebecca, then Barbara.

DR. MERCURI:

Well very quickly, mine is very quick.

MR. RICHIE:

Well this was said in our testimony but I'll just summarize it quickly, which is, what a great help to jurisdictions that are going to rank voting methods and cumulative voting systems would be to explicitly address the standards for doing so. And there are some good precedents out there; the State of Minnesota has a task force. Our Secretary of State, Mark Ritchie has come up with, you know, examples of what these standards might look like and I think that that would be very valuable because right now it's heading toward another set of standards that will leave jurisdictions in the same very messy place where they have been, where they are trying to

do something that the vendors aren't clear how to do it and having invested in it and then are being told to do it and they don't do it well or they don't do it at all and so there is road maps to get that done. Also, I don't know if there are -- and we have some specific suggestions of where that would go in.

The issue of ballot images and optical scan systems and having that redundant way, in a sense to check potential fraud with paper ballots, if you think of software independence, it's almost like something that's independent just of the paper ballot if we think there might be potential corruption and fraud with paper ballots. But there needs to be standards addressed for when to use those as the audit trail.

DR. KING:

Okay, thank you. Rebecca, and then Barbara, and then John.

DR. MERCURI:

I still believe very strongly that if the VVSG was changed to be a true functional standard, as opposed to a design standard, as what I believe it now is, that that would significantly decrease the cost, time, and expense of doing the testing. That's my belief, but I think I have some grounds for that.

Also, I had previously, for an earlier event in December, identified what I called the under addressed issues in voting systems standards and it's just a one page bullet point list, so I'll make that available into the record.

DR. KING:

Okay, thank you. Barbara and then John?

DR. SIMONS:

So, in my testimony, we have a list of ten recommendations and suggestions. I will not read them off. There are just a couple I wanted to highlight, one very general and one very specific.

The general one has to do with electronic poll books, because these things are being interfaced to voting machines and of course, the whole elections problems in these poll books, which I expect we will see a lot of in November, can have a serious impact on the election, so I would just like to suggest that the EAC consider expanding the definition of voting systems to include electronic poll books, especially when interfaced with voting systems. I realize this is going to create a lot more work for everybody and that's not my intention but I think it needs to be done.

Now going down from the very general to a very specific suggestion is the notion of failure rate for voting systems. As I read the VVSG, failures are all lumped together in computing the failure rate, but as we know, some failures are better than other failures. They're not all equal. And, you know, to paraphrase George Orwell, and I think they have to be taken into account. This is -- there are real problems with using that as a measurement.

DR. KING:

Okay, thank you. John and then Larry you get the last word before lunch.

MR. WASHBURN:

Okay. Well I'm not sure this is a specific recommendation to the VVSG, but that larger framework with the program manual and the NVLAB Program, is that, we've kind of reiterated over and over

again, you know, that voting takes place in a very complicated political, social, and legal environment and technologies at best, the tail of that process.

So I guess, what I'd like to specifically ask is, that either in the program manual or part of the VVSG or as part of the NVLAB Program, a mechanism by which the technologists could make a recommendation back to the EAC for legislative aids that might help with administration. And the example I included in my testimony was, for example, with Sarasota, Florida had their vending requirement that for federal elections, you must have a write in, you must have, none of the above, no candidate is acceptable, none of the above, any candidate is acceptable, and require a mark for all of, you know, for at least one and no more than one. If 18,000 votes come up short, you know that's machine fault. At least, it lets you segregate the question. Is it a machine fault or is the voters have decided not to vote? Those kind of feedback back to the other parts of the voting process, the legislative, the social, and the legal, is absent in this little -- but I'm not sure if it's the VVSG, the program manual, the NVLAB, or just part of the EAC reporting requirements. I mean, there's no mechanism that, we're talking about feedback. There's no mechanism for feedback to those other aspects of the system that are not technological that might help mitigate or reduce technological issues.

DR. KING:

Okay, good, thank you. And Larry?

MR. NORDEN:

Okay. I will be quick since I'm standing between everybody and their lunch. One thing that I would like to see added to the VVSG is requirements for the audibility of voting systems. Software independent voter verified records aren't worth all that much, from either a public confidence or certainly from a security perspective, if they're not being used. And I was just in Ohio helping them out with a post election audit that they were doing there and, you now, these systems vary a great deal in terms of how easy it is to use them to conduct audits. And I think it would make everybody's, certainly election officials lives, a lot easier if they had systems that not only had software independent records but software independent records that they could use straightforwardly to conduct audits or recounts.

DR. KING:

Okay.

MR. WASHBURN:

And I just want to make clear that none of the above recommendation is not the position of Voters Unite or even really mine, it's just an example that I could think of that would...

DR. KING:

Okay, thank you, John. Let the record reflect...

MR. WASHBURN:

It's not like I'm going to be pressing Congress and they go, oh, you got to do this.

DR. KING:

Okay. Well before we adjourn for lunch, first, let me thank every member of the panel for your input this morning. I think we've had

an excellent discussion today. Again, I'll echo something Mark said. I learn a lot from every one of these and so, I do appreciate the preparation and the sharing of responses to these questions. When we come back from lunch at 1:00, this will be an opportunity for each of you of the panel, to summarize what you said earlier, to reinforce the points that you think are important, to go back and maybe address something that over lunch you thought about, that really needs to go into the record and be shared not only with the other members of the panel but with members of the EAC here. And what we'll try to do is allocate about five minutes to each person's closing statement, if you will, and we have an hour to do it and we've got nine people so, if we can keep on track with that that would be great. There restaurants and fine dining completely surrounding this area. I want to note there is sandwich shop across the street and McDonald's down at the corner. Perhaps some members of the EAC staff could give different or alternative recommendations, but I would like to reconvene right at 1:00 in this room and be ready to go. Thank you.

***

[Luncheon recess from 12:04 p.m. until 1:09 p.m.]

***

DR. KING:

Okay. I think we're ready to resume our roundtable discussion on the VVSG. As I said before lunch, this is now an opportunity for each member of the panel to kind of summarize their thoughts, drive home whatever points they think are particularly significant that we need to retain or reflect on. And what I'm going to ask is

that each member try to limit their comments to three to four minutes and if you see me holding up a finger that means you've got one minute left, to kind of wind it up and I do want to try to finish by 2:00 because I know we have some people that have appointments after 2:00. We're going to start with Rebecca and we're going to work our way around the table and eventually we're going to end with Brian who, as the EAC representative on this panel, as host, will get the last word in this regard. So Rebecca, if we could begin with you?

DR. MERCURI:

Okay. I think this one is dead because it's light is off on the front so. It's dead. Okay, all right, got it. Well I have two dead. Okay, very good. Well I want to touch on a few things that we may have eluded to but didn't really get into, but primarily, my concerns are the -- that this process is leading to, rather than solving the erosion of voter confidence in elections. And I really feel very strongly, that the process, since it is not really providing the true assurances and especially, transparent assurances of process or equipment correctness. It doesn't mean anything to me at all that the voting machine is certified and that this particular version has been certified, if it is possible for a community to have installed the wrong version of the software or the firmware or whatever in the voting machine and they use that for many elections and it never gets detected unless somebody has a FOIA request, they're never going to find out what version is in there.

As an anecdote, but a truthful one, I was involved in a recount, that's actually still going on being contested in appeals in

Ohio, in Franklin County, Ohio, related to a judicial race in the 2006 election. And one of the things that I was able to discover, again, after numerous FOIA requests, was that in Franklin County, they had deployed a configuration of the ES&S iVotronic and with a paper trail but we'll get to that in a second. But they deployed this configuration, that it was sort of some from Column A and some from Column B. They had taken two certifications for the iVotronic and there were a few components, there was like ten components so, like, some were from one and some were from another. And as we know, those certifications, the EAC certification says, for this configuration and the configuration is specified, so it was a violation of that and it was also a violation of state law, which said that, it had to be a certified configuration.

Now why do we care about that as computer scientists? We know that if you swap out one part and put another part in and it hasn't been what we call, integration tested together, then all bets are off. We don't know whether those components actually will work together correctly. So in court, we wound up in hearing ES&S claim and we have no evidence, you know, one way or another that they had tested it and it was okay in that configuration. But that's not what the system is supposed to do. And again, the transparency, there should be a way of knowing that this is the properly installed configuration.

Now unfortunately, what also happened in that case and again in other cases that I've seen of this type is that, then the person contesting the election had to then prove that somehow that configuration affected the outcome of the election, despite the fact

that in that particular election, the county admitted, again, after our findings also discovered this that, in fact, over 80 percent of the precincts had a different number of ballots listed from the machines, as there were voters who had signed the polling books. So this is in the extreme. You have anomalies where people say oh, we're going to audit the election. Well we audited it and we found that 80 percent of the precincts had a difference in the number of ballots. I'm not talking the vote totals, I'm just talking the physical numbers of ballots themselves and, you know, again, this was a DRE with a paper trail and I'll get to the paper trail in a second. But again, if that audit occurs and there is no way of doing something about that audit and again the, you know, in court, the person contesting the election has not proven, you used the wrong configuration of voting machines, 80 percent, I think it was 84 percent of your precincts are off by numbers and some of them were even in the hundreds of the number of ballots that -- and they're required to prove this, in the absence of being able to test the machines and they have to prove that that somehow affected the election. As far as I'm concerned, that should be enough sufficient proof right there. The Judges are reluctant to rescind a result. And what we're seeing is that, the result generally stands. Whatever the result is that's given on election night, people are unhappy about changing that.

And one of the problems I want to talk about, just, you know, since in my last minute here, is this business of the voter verified paper ballot or, you know, the audit trail. And there were VV pads [ph], they were the reel to reel kind. And, in fact, the contester had

paid for 3 percent of -- well actually, he had paid for 50 precincts, which actually was slightly less than 3 percent of the county, to be hand, recounted from the paper ballots. And the rule from the state said that 3 percent, in the recount, 3 percent would be counted but you have to pay for them. So he paid for this.

And so, what happened was, that then they decided that, no, we're going to count the ones you paid for, we're going to count other ones you paid for, 3 percent of those. No, not 3 percent of 3 percent, it's 3 percent of all of them. And so, the VV pads are worthless and the audit is worthless, if the audit is not done appropriately. It's not done statistically. And if there's no rules, as to what happens when you do have a variation, what are you going to do next? And that's -- these, all of these things that were, remain to be totally unresolved in, you know, in the voting system guidelines. We don't have anyway of mitigating any of this and the transparency is just not there. So these, you know, from the real world, this is what the voters are seeing and the confidence is just being eroded. So those are my summary remarks.

DR. KING:

Thank you, Rebecca. Rob?

MR. RICHIE:

Thank you. And again, I've learned a lot today and so it was a real pleasure to hear all the comments today. I think I was talking to Rosemary Rodriguez just before we reconvened and in talking about how France had 87 percent turnout and they don't have absentee voting and they had all these point place elections and, you know, and didn't seem to have a lot of the problems that we

have. And she did point out that, they probably were voting on two things, while we're often voting on 80 things, at least in some of these places that have so much to vote on.

There are certain challenges for the U.S. that we have to keep in mind about, you know, the number of jurisdictions, the number of elections, the numbers of offices we have that are just, you know, kind of immense in international norms. But also, part of that is, you know, that are a lot of international norms that -- on a lot of the parts of voting process, I think, are better and I think that Americans want to be number one in things. I hope that we can sort of keep after it and try to get the best system and, you know, that issue of getting the resources that we need to do it, I think is one that we have to keep in the forefront here and when we get to positions of tradeoff because we're not investing in the system however we should. We do generally run elections on the cheap in this country compared to what a lot of other places do and I think we should not do that.

Just to, you know, beat the horse but not to try to do it too much. I mean from my perspective is, our system is highly vulnerable, you know, when we have voting systems that allow that vulnerability to happen. So as soon as we start talking about spoilers and third parties as we will shortly with, you know, Bob Barr might run as a libertarian and Cynthia McKinney is agreeing, and Ralph Nader's running, those kinds of elections, it's because our system is vulnerable to it. Jurisdictions are trying to deal with that vulnerability with instant runoff voting and clash with the process that has been established for running elections in this

country. And that's something that I think, that I hope these standards because the standards play a key part, as written now, this will not help jurisdictions, really, almost at all with the challenges that they face, when trying to get majority voting through instant runoff voting and fair representation through cumulative voting and single transferable vote, which they often do in voting in the United States. And I think that we need to, you know, make sure that is not getting in the way of that happening.

And I think that, so the point I was making earlier, about, can we make flexibility a standard some way or anticipation of a potential public interest needs, some thoughtful process which got back to John's point early on, do we really know what voting is, that we really want voting to be in this country? Have we had that bigger conversation and when do we have it? And then how does that relate to being able to implement these decisions? And certainly, when the challenges that we face often, are when a jurisdiction is trying to do something different, it clashes with the profit incentive of the companies, the vendors, and there's an institutional resistance that is founded on not anticipating these public interest potential changes that these jurisdictions have decided on, in the public interest.

So, I hope we can figure out a way to kind of address those. And the specifics we care about are voting methods but that's not the only one. There are other voting methods that are worthy of consideration and I'm sure that it's a window into other things that we may want to have incorporated into voting that end up getting

blocked because of rather rigid regime that gets set up for voting equipment standards, thanks.

DR. KING:

Thank you, Rob. Lillie.

MS. CONEY:

Thank you. This has been a very good discussion and one that I think is something that is a long time in coming and how do we move from where we were to where we want to go? And I want to congratulate and offer my appreciation to the EAC for being such a good steward of the discussion process leading into the latest version of VVSG that will be rolling out and we'll be working with over the coming years and maybe struggling a little. We'll just see how it all works out.

But I wanted to point out some things that was coming from this discussion and some of the work that I do over at the Electronic Privacy Information Center that we think is very important. Data on election technology should support transparency, but it should not threaten voter privacy.

And there's another aspect of transparency. We didn't get much talk on this today. We talked about it a little bit and but very succinctly, cost transparency to local and state election jurisdictions. What am I paying for something, versus what another jurisdiction is paying for it? Literally seeing the costs broken down item by item, including breaking out election services and what those costs are, so you can shop more effective consumers if they know what the costs of things are that they're buying and maybe create some transparency on that for elections officials may be

helpful in dealing with some of the cost factors that are -- impact the election process.

And creating the matrices for collection of data, so that it's usable and it makes sense and asynovizing [ph] reporting incidents too, from local polling locations to the state and the state onto the federal government. As you know, polling day practices are basically from people who are willing to go and volunteer obstensively, although there are some financial compensation for doing it, but adding to that burden of what they have to do on an election day, we always have to be sensitive to that. But the competing interests of collecting data will help better inform the process, the standards process, the testing process, and working on some of the hard problems around voting and elections for voters.

Looking at elections, another point that's very important is, elections should be voter centric. They should be able to serve the needs of the voter. The voter demographic is just, it's very difficult to define because it includes so many people of varying abilities and disabilities. And this also should incorporate what we see from poll workers who are representative of the communities that they will serve.

And thinking of those terms, I saw one thing in the VVSG referring to the knowledge of using ATM machines, that people feel comfortable doing that, but that's a socioeconomic assumption, that there are ATM machines in most communities around the country and there are some urban areas where there are no ATM machines, there are no banking -- the experience for those voters

will be very different, if you take the assumption that everyone knows how to use that very common technology that we see in most of our lives.

The other issues around cost of R & D and costs of election administration, these are real issues that are public. The elections are public -- of public interest. They are also of public good. And the discussions of costs and how do we meet those costs are far outside the reach of the EAC but they have to be a part of the discussion. And as part of the processes of the EAC doing this, I would also suggest that you bring in people who would talk about how do you factor in the costs? What are the costs for doing the things that we'd like to do? Doing the things we think we ought to do and so we can get some real numbers on that including R & D issues, not just from the vendor perspective, oh, it's going to cost a gazillion bucks if we have to redo this, but from quantifying it in ways that can create a matrix that can be a lot more available to policymakers in trying to make decisions about how much resource should be put into the process and what's reasonable per voter, compensation to local and state jurisdictions for conducting elections.

Looking -- and this is the real issue with voting, being voter centric. You have 12 million registered voters in the State of Texas. You have over 9 million registered voters in the State Pennsylvania. Voter registration rose statewide, are in the millions. To really, realistically think that we can process all of these people on a single day, who could do that? Who could possibly do that? How do we fix or develop or start moving toward a system that can have a

reasonable expectation of serving the community it's supposed to be focused on serving and is that possible? Does early voting get you there? Does remote voting get you there? And then taking into all these possible ways that you could cast ballots or participate in a public election, you have to bring in all those competing interests about security, reliability, auditability, transparency.

These competing interests create an environment that is so unique, so different from any other human venture because we're talking about it on a scale that is just unprecedented. And a lot of countries around the world, it might rival our population in a popular democracy, aren't really that good at democracy. And there are some that have had, even in their development and evolution, that's happening in democracies around the world, but the more populous democracy like the State of India. The election they had in 2004, there was a discussion of a great improvement over previous elections because election violence was a real part of their history. And so routinely 600 election related deaths were not an overestimate. They had under 100. They've had great success. To our conscious and to our sensibility about elections, any, would be just a shock. You know, it's just something we would not even consider. But when you're talking about mechanics of elections, millions of people participating in the process, that the process has got to actually have some chance of serving those individuals, we're just starting the conversation about how we're going to actually accomplish that.

And in the other aspect of elections, recognizing the beginning of the conversation that, incidents happen, incidents

should be reported. But what do you do when you get an incident? Should we have something akin to other agencies like the National -- the Department of Transportation or the Food and Drug Administration incident being reported is evaluated based on a set matrix and depending on the threat to the underlying goal of the whole reason for that institution existing, there's a reporting team that goes out there and certain things that are going to take place. And it's not a matter of someone's out to get someone.

The valuation process may not be able to inform the final decision in an election because it may take a while for it to actually follow through. The goal is to learn from the incident how to make the system better, so it's a feedback mechanism not a judgment scheme on how to place blame. And how do we create something like that, that works in tandem with testing and certification, is something that may be helpful.

And the last point, which also serves elections, which also serves voters, is fail-safe election strategies. Elections are very difficult to get 100 percent perfect all the time. So, if you're going to try to think in terms of elections and a set designated day and time, you don't get the next day to do it right or do it again. And how do we have these conversations around, if you show up to vote, you should be allowed to vote. It shouldn't be a factor of the machine's not working or that the poll worker not being ready or some of these other things not being in place. Can we, in fact, have those kinds of discussions, around making sure the process works, based on the time frame, the legal framework that's out there for it to work, and what makes sense to try to accomplish those things, taking into

consideration the work of election protection efforts by elections administrators, usability, accessibility, security, cryptography, process, procedure, audit, oversight, accountability, and of course, from our perspective, the most important is, privacy of voters. Thank you.

DR. KING:

Okay, thank you, Lillie. Barbara.

DR. SIMONS:

Thank you. Well first I want to say how pleased we are that the, excuse me, I tried eating lunch too fast. That the EAC is holding these roundtables and we very much appreciate the invitation to be here. I personally appreciate it.

Lillie talked about people dying in India with their elections. Certainly I remember and I expect most of us sitting at this table remember when people used to be murdered in the United States for trying to exercise their right to vote. This is a sacred trust that we have, to try to make these elections as good as possible and we owe it to the people who sacrificed their lives for this right.

So, and I agree with Rob, that we are trying to do elections on the cheap. And it's most unfortunate and it sort of contradicts what we were just saying about people giving up their lives for this right. We have run elections in this country in a way that we would never run our businesses. We would never have a business, especially an important significant business, which never conducted any audits. Where there was no way of holding anybody accountable for what happened and yet we continue to do that with our elections. We must have elections that are easy to audit and

we need to do audits and we need -- I mean I realize that the EAC cannot make legislation but I think this is something that we all need to keep in mind, that we need audits for the accountability. And when I say, easy to audit, I mean, for example, The V pads that we have on DRE's which are better than DRE's with no V pads in general, are not that easy to audit. And it's still the case that the easiest thing to audit is going to be paper ballots, voted by the voter and we would hope that the EAC would push for durable, easy to read and verify, paper ballots.

The most cost effective and fail safe technology still, is precinct based optical scan, where the voter marks the ballot and puts it through a scanner to check for over votes, possibly under votes, and other marking problems. And then, of course, for people with special needs, such as visual impairment, language other than English, there's good ballots, that the best technology still is ballot marking devices capable of producing paper ballots that can be independently scanned for voter verification, error checking.

Given these goals, we think it's critically important to support software independence, independent voter verifiable records, and open ended verification technology, OEVT with the caveats that I mentioned in earlier discussions, that we do have this tradeoff issue, which is why we need audits because that's a way to deal with the tradeoff issue.

The VVSG is a -- the Draft VVSG is a huge step forward from what we've had before, its huge. And we do appreciate all the work that's gone into it. Our plea is to, please implement it soon. Please implement it soon, don't take it apart, keep it the way it is,

maybe make some corrections to it but keep those basic concepts in it. Get it out there. We're going to have problems for a long time anyway because we've got these old systems still out there, which have not been certified, to the standard of the 2007 VVSG. We need to start really fixing up our elections as quickly as we can. Thank you, very much.

DR. KING:

Okay, thank you, Barbara. Zinelle.

MR. OCTOBER:

Thank you. I'm really pleased to be here on behalf of NALEO. These are very important issues we've discussed today. I've certainly learned a lot. I told you I didn't really have the technological or technical background but certainly have a lot to offer and certainly received a lot as well.

So, I guess to summarize overall, what has been my takeaway from this, is something that Barbara actually summed up pretty well I thought, when she focused earlier on usability, accessibility, and security, as kind of looking at all of those items throughout the entire process, not at one point, what can we get rid of, competing interest, they're all equally important. Another really important thing I think is, keeping this open and transparent. We have spoken about that on various levels here.

I mean, we have to gain the trust of the voters. The voters are who count ultimately, in all of this. And we're at a point now where people are registering more. We've had a huge campaign at NALEO through our Ya es Hora campaign, where we've increased registration in great numbers and we want to continue that. And we

don't want to lose this enthusiasm we have with the voters now and one way not to lose them is to increase voter confidence. Let them know that when they go to the polls it will be easy to use these machines. It will be easy to cast your ballot. It will be counted through reliability and security. We have to keep this momentum going. We just can't let that go.

I appreciate all the efforts that the EAC has taken and I think forums like this, if you continue along the way and include advocacy groups along the way then, you know, we have a lot to offer and I think it will only get better but we have to all work toward that.

DR. KING:

Good, thank you, Zinelle. Larry.

MR. NORDEN:

I would also like to thank the EAC for holding this roundtable and other roundtables. I really do think that they are an important and useful exercise and I also have learned a lot from being here today.

I want to reiterate a couple of things that Barbara said. I think that this Draft VVSG is a huge improvement, in terms of, on issues of security. Something -- it's unfortunate we didn't really touch too much upon issues of usability and accessibility of the voting systems and I think for many voters, those are really the most important issues themselves. And we are here as advocates on behalf of voters. I would say that this VVSG is also a great improvement in those areas over the previous VVSG. And for those reasons, I would also echo what Barbara said. I really, although I think, you know, there are certainly some improvements

that could be made. I don't want to see this; the implementation of this VVSG delayed any further.

I think one of the things that there seems to be agreement on at this table, that there probably should be agreement with everywhere is, that even though these guidelines are better, we're never going to have guidelines that are going to get us to a point where we have perfectly secure or perfectly reliable systems. That's just not possible. And that's why I would come back to the importance of software independence, of allowing audits, so that we can check to see if there were mistakes on the voting systems. And the importance of the feedback loops that a number of us have talked about before. And I would say again, that's not just important for issues of security and reliability of the systems, it's also important, feedback loops are also important for improving access and for improving the usability of the systems.

One thing I wanted to touch upon, we actually didn't get to the very last question that was asked and since the election officials are going to be here tomorrow, I wanted to -- the last question that we were asked was, how the process of developing and vetting the VVSG could be improved to ensure higher quality input from election officials. I have an answer to that and I think it would also help improve voter, general citizen understanding of the VVSG and input on the VVSG. I think for both, for election officials and for voters, probably the most important question that they would have about the VVSG is, how does this affect operations of elections? How is this going to affect from the voter's perspective what

happens when I get to the polling place and vote? And for an election official is, how I run my election.

And I think it would be helpful for comments from those groups. If an organization like NIST or NASED, or maybe those organizations working together, were able to put together some kind of operational checklist that allowed election officials and citizens to understand how each technical specification, either would or would not affect the voting process and the administration of elections.

DR. KING:

Okay, thank you. John?

MR. WASHBURN:

Thank you. I'd like to thank the EAC for these roundtables. It's a lot of roundtables and a lot of very heterogeneous groups that you've pulled in, to hear from. And I'd also like to thank the National Institute of Technology. The new VVSG represents a lot of work.

I guess, in closing, Voters Unite, in particular and myself even -- we have difficulties believing that the standards will be implemented and enforced. The past ones haven't, so past is usually your best guide to the future. And one of the things that has come up and I would reiterate is, that idea of feedback. In a typical software development process there is a great deal of feedback between, you know, the test group, the development group, and the usually, it's some business analyst or some designer, you know, between those three groups. And there's no analogous communication pass in the election environment. I mean, I would

argue that the election officials are probably your designers because they know what they need to do to make that voter centric experience. So the feedback is a significant problem and the EAC, I believe is mandated by HAVA to be a clearing house for specifically, that purpose is to help facilitate that communication between these disparate stakeholders in the election process.

Mr. Hancock mentioned specifically, the quality monitoring program that's been implemented and I have real problems with that being the official mechanism because its definition of anomaly is so narrow, that nothing gets reported -- my fear is that, absolutely nothing reported by an election official, no matter how grievous, will make it meet the definition of anomaly. Anomaly is defined as, an irregular, inconsistent action. This is Section 8.73 of the Voting System Program Manual, Testing and Certification Program Manual. Defined as an irregular or inconsistent action or response from the voting system or system component, resulting in some disruption to the election process. Incidents resulting from the administrator error or procedural deficiencies are not considered anomalies.

Now, my problem is, is that this is a very high bar that is very unlike any other engineering process, where there idea is, report everything we'll sort it out later. Even if you -- if the track is trivial, not reproducible, it's accepted that there are reports that are spurious, but take them anyway, because, ironically, sometimes the most spurious reports, that intermittent problem, has actually manifested itself. So with this particular definition, it's possible to have violations of the VVSG, which do not result in the disruption of

the election process, not an anomaly. That would just never get reported. The only people who have standing to make such a report are election officials.

So, taking for example, September 14, 2006, in the City of Milwaukee, I videotaped that the scanner's LCD display, of total number of ballots cast, did not match the number printed on the report, so the machine was internally inconsistent as to how many ballots went into it. The simplest statistic it's supposed to track. And neither of those numbers agreed with the number of ballots that they handed out to electors, according to their paperwork. Well I have -- again, I have that documented from the official records and from videotape. And even if my local poll worker, you know, the election chief wanted to report that and wanted to violate the omerta [ph], as it were, of election officials when it comes to voting anomalies, that may or may not meet the definition of a disruption to the election process because it was only off by 10 out of 500, you know, probably didn't affect the outcome. I'm -- I can see that rational being used.

And similarly with the Sarasota election, the supervisor has been blamed that she laid out the ballot badly, on the touch screen. Well that's an administrator error, even though it lost 18,000 votes. And those are just two recent examples, I suspect, if I applied this filter to everything that came up in Pennsylvania this Tuesday, every one of them could be ruled as either non-disruptive, administrator error, or procedural defect. What gets into the system then? So, even the feedback system that's been established to help guide the VVSG, as the handbook says, you know, based on

these reports, NIST will take a look at improving the standards in the future, there will be nothing there. It will be an empty sack.

So I have -- we -- Voters Unite has problems with the past performance of the EAC and it's clearing house rule and specifically some of the details of how it plans to be -- fulfill that role in the future. And so again, it really erodes that transparency and the feedback and just the general presumption that we -- if there's a problem that we should follow the evidence wherever it should lead.

DR. KING:

Okay, thank you, John. Mark.

MR. SKALL:

Thank you, Merle. So I as well would like to thank the EAC and Merle for hosting this, giving us all a chance to say our piece. Of course, since I and Brian get to say our piece many times, probably an unfair advantage.

Voting is really crucial. Voting is crucial to democracy and thus really deserves special attention. There are other systems in society that deserve special attention and are given special attention, such as mission critical systems, where loss of life is very possible. Mission critical systems typically use an order of magnitude or many orders of magnitude, more resources, more funding than is funded by voting systems. So, like someone said, we are sort of funding this on the cheap when you compare it to other important things in our society. If you had more funding like many of these mission critical systems do have, you can do some more things to make the system better. Some of them use formal

methods to a greater degree, which may help, aerospace builds in redundant systems. We don't have enough money to do that.

So, in voting though, we have very real world limitations. There are budgets that have to be operated and there are very real world problems, no identification of the voter to the transaction, no receipt, et cetera. So, I think the conclusion of this is, that voting is hard. It's really a difficult technology and we have to realize that. So what can we do? So we have to start by developing the best standard we know how. Everything revolves to me around the standard. Tests are all important but unless you have precise testable vetted standard, you have nothing. So, this is really a necessary but not sufficient condition to where we want to go.

If you have a good standard, then you have tests and certification procedures. Again, I've heard mention around the table about the proprietariness of various tests. That's something that we are addressing, again by having a test sweep that we're developing that will be, not only we believe, comprehensive, but completely transparent, so everyone can see what's going on in the process. I think that will help.

When it comes to risk assessment again, a very worthy effort but we need to try to include different people from different disciplines, because I think it won't work and perhaps we need to lower our expectations by what we're going to get out of that.

One other thing I do want to address. I've heard a lot of mention about design standards in the VVSG. And let me just sort of go over the types of requirements that are in any standard. You can have functional requirements, which basically talk about what

the system has to do. You can have performance requirements, which talk about what the system has to do and how well they do it and specify benchmarks. You can have design requirements, which essentially prescribe how that has to be done.

In a perfect world, we've all agreed design requirements are not as good, but let's remember there are many competing factors here. All of these requirements have to be testable. So we can look at, so the functional requirement by something that needs to be readable. That's a very good functional requirement. But when you look at it, something needs to be usable, it maybe that when you try to break that down into testable functional requirements, you can't come up with any, but you can come up with good design requirements that are well accepted and have been well vetted, such as, fonts must be a certain size or icons should look like this.

So there are many times when you have to have design requirements. They are, in my opinion, better than nothing, when you have a high level functional requirement that can't be tested. We all agree you have to have testable requirements so there's a tradeoff here, but it's not all that simple. Thank you.

DR. KING:

Thank you, Mark. Brian?

MR. HANCOCK:

Thank you, Merle. Again, on behalf of the Election Assistance Commission, our Commissioners and Executive Director, I'd like to thank you again for coming today. It's been a great discussion, as all our roundtable panels, frankly, and we appreciate the feedback from everyone.

I will just remind you again of a couple of things that I noted earlier. Please if you haven't done so, post your comments to the VVSG by May 5. You know, the web portal is up there and we hope that you use it.

Also, I just wanted to say something that hasn't come up today and it's sort of my fault for not mentioning this earlier, but I want to remind you of the election management guidelines that are being produced by the Election Assistance Commission as well. They are essentially a companion document to the technical guidelines that we've been talking about today. I think, as we all know, you know, even though that's what we're focused on right now, the machines are only a very small part of the election administration process and they're even -- there's been a lot of talk today and stuff that's sort of peripheral really, to the machines and more related to the practices and procedures.

The documents that we're creating are essentially putting forward best practices from across the country, to be available for election officials to use, if they want them. As we all know, funding is an issue in election offices. There are a lot of small offices that don't necessarily have the time or the people or the money to develop these practices for themselves, so we're putting them out there. Hopefully, everyone will use them.

They're touching essentially on all aspects of election administration. They talk about state certification, accuracy testing, contingency disaster planning, developing an audit trail, and numerous other areas. Our quick start guides are little manuals that we've been mailing out, are out in the lobby right there. If

you're interested, please feel free to take some with you and distribute them as you see fit. But we're very proud of that document and it's been very well received by both election officials and representatives of the public so I just thought I would remind you of that as well.

Once again, thank you, and thanks to Merle for your great job once again, moderating.

DR. KING:

Thank you, Brian. Well I'd like to make just a few closing observations, as I do at the end of each roundtable. And I find this useful, particularly to myself, to kind of reflect back on what I've heard today, but I think it's also useful for the group as a whole to recognize really how much ground we did cover in four hours today. So I'd like to share with you some of the things that I heard today and ultimately will be reflected back into the deliberations of the EAC.

I heard that there are existing methodologies that have been already vetted, the common criteria that could be looked at, as a source for integration into the VVSG. The pursuing risk assessment, a laudable goal, but should not in and of itself delay the implementation of the VVSG. That not all risks are created equal and that those that have the highest impact, possibly the alteration of an outcome of a state election are perhaps the most egregious. That voting is a national security issue. That it should be perhaps elevated in the consideration of national priorities. That wholesale election fraud should be considered a significant risk, as we more and more rely upon computer systems even with paper

based systems for tabulation. That the solutions that are implemented, as a result of the VVSG, should have high face value to the voters, the ultimate stakeholder in these systems.

That a risk forum for the other components related to the voting system, I think the VVR, I'm sorry, the VR, voter registration systems was mentioned. That we need, I'm sorry, that, if we need a special innovation class within the VVSG as a way to accommodate new systems, then perhaps the VVSG needs to be re-looked at, to accommodate that without special provisioning. The risk assessment should precede any compromises in the functionality or other goals of the system. A question about, should R & D be handled by the vendors? Is it so important that perhaps R & D should be shifted over to a public funding venue?

That regarding the OEVT, that perhaps expert system review might be a better descriptor of what was intended in the draft of the VVSG. A clearer understanding of what is done with defects that are discovered in certified systems, that are still within the scope of the specifications of the certification. An observation, that testing will be only as good as the testers and the methodologies that they use. That the -- I'm sorry, uniformity in test criteria used in the open ended voting, open ended vulnerability testing, I'm sorry, is an important criteria.

See the process changed for how voting, I'm sorry, how test labs are selected and their services paid for, perhaps a change in the funding model. That, expansion of the standard to include usability, greater usability emphasis should involve advocacy groups. That, a well-designed system should integrate usability,

accessibility, and security from the initial design phase without those compromises being forced onto it downstream. Look forward to the need to include ranked choice voting methodologies into the standard. That, we need true functional standards rather than design standards reflected in the VVSG. That, electronic poll books may well need to come under the scope of the VVSG in future iterations, given their integral nature to the voting process.

That, the VVSG must avoid the risk of contributing to a lack of voter confidence rather than increasing voter confidence. That, there are international norms that the U.S. could learn from. There are improvements that have been made in other nation's voting systems that may well add value to U.S. systems. That flexibility within the system, within the VVSG, is a desired attribute, that is, its ability to accommodate unanticipated improvements at the time of approval of the VVSG. That, cost transparency is an important dimension of the transparency of voting systems. Jurisdictions understanding the true cost of a system in terms of maintenance, use, et cetera. Incentivising, and there's a new gerund for me, that, incentivising election problem reports, as a part of better data, election collection, and then feeding that incident report back into the certification and the process. The cost of research and development and the cost of elections administration is an important public issue.

That competing interests increase the complexity of administering elections that cannot be an excuse for not striving for greater improvements in election administration. Improve the feedback system on incidents to interface better with the

certification and testing process. That, systems must provide ease of auditing, specifically, must produce durable and easy to read optical scan values. That, software independence, open ended vulnerability testing, and IVVR are desirable goals of the new VVSG. That, usability, accessibility, and security, integrated from the ground up in design avoid creating conflicts down and avoid the creation of a zero sum strategy, where we have to give up good things to get other good things.

The EAC should avoid unnecessary delay in implementing the VVSG. The VVSG needs, and I forget who said it over here, the equivalent of an environmental impact statement, that, when it is put into play jurisdictions need an understanding of how it will impact their operations.

And that is my summation, of really, I think, an incredibly productive exchange here today. And I want to thank the Commissioners of the EAC for sponsoring this. I want to thank Brian and his staff, Matt, who's here, really, for an excellent job of conceiving of these and putting them together. And, has been my practice, we will adjourn this meeting right on time at 2:00 and with that, the meeting is adjourned. Thank you.

***

[Whereupon, the roundtable discussion adjourned at 2:00 p.m.]

Written Testimony by Rebecca Mercuri
mercuri@acm.org 609/587-1886
Representing: The BRAD BLOG
Voting Advocates Roundtable Discussion
EAC Offices, Washington, DC, April 24, 2008

The 2007 draft Voluntary Voting System Guidelines (VVSG) represents a significant departure from earlier Federal voting system guidelines (2005 EAC, 2002 and 1990 FEC), while still retaining much of the certification framework that has been increasingly demonstrated to be problematic. Within the guise of certification, the past few years have seen billions of Federal and State tax dollars squandered on the purchase of voting systems that were subsequently revealed as inappropriate for use, and then discarded. We now know that the VVSG, and its ITA testing program, provide no assurance of process or equipment correctness, either to those who are making procurement decisions, or to the citizens who must entrust their votes to these systems. Tragically, the net result of this false validation has led to further erosion of voter confidence in elections.

This draft VVSG continues to perpetrate this scam. Among other changes, it recognizes earlier shortcomings of the certification process (especially in the areas of voter verification, transparency, auditability and security) by introducing an innovation class that allows for the submission of novel voting system paradigms for certification, and provides for the (somewhat related) adoption of a software independence requirement. Unfortunately, both of these concepts are oxymorons in the context of voting system specifications. Here's why. If a construct is truly innovative, the existing guidelines will not be able to appropriately address it, hence the resulting certification may be flawed or the implementation of the new design may necessarily be impeded by a lack of understanding as to how to properly perform certification. A system that contains software can never be software independent, even within the TGDC/NIST's constrained definition that ties undetected changes or errors in software to election outcomes. Any software in the system necessarily affects a whole host of voting attributes that can affect election results, irrespective of undetected changes or errors.

Furthermore, neither the innovation class nor the software independence requirement are satisfiable due to legacy constraints imposed by the certification process. This is, at least in part, because the 2007 draft VVSG (like its predecessors) masquerades as a functional standard, while actually continuing to be predisposed to existing designs. Even the TGDC's description of the innovation class makes design assumptions, such as its limiting "expect[ation that] most technologies in this class [will] be based on multiple mutually auditing components." But even as a design specification, the draft VVSG falls short of achieving its goals of specifying "how voting systems should perform or be used in certain types of elections and voting environments." This is because the guidelines repeatedly make the erroneous assumption that insiders (i.e. vendors, repair personnel, election officials, etc.) are trusted agents in the highly partisan process of US elections. In reality, insiders have both motive and opportunity to make changes and cover up the fact that they have done so. Where errors have been blatantly obvious, vendors go to great lengths (including lawsuit threats) to prevent independent examinations of equipment architecture and computer code. Some election officials have improperly conducted audits in order to avoid revelation that problems have occurred "on their watch." In sum,

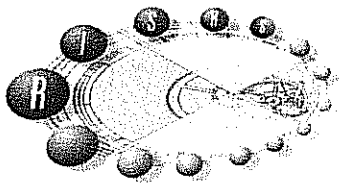
virtually all of the checks and balances that are specified by the VVSG fail to take insider attacks into sufficient consideration. Voters believe that elections are inherently corrupt, and the VVSG does nothing to allay these fears.

Nor are the VVSG's specified controls transparent enough to allow verification by the voter that the election system they are using has been configured properly. Production of a voter-verified paper ballot is utterly moot if vote totals are generated electronically and never checked against the original paper. Recent literature has suggested random audits (or spot-checks), but since these percentages are based on the computer-generated results, they grossly underestimate the amount of independent tallies that must be performed to sufficiently validate the election. These checks are not prescriptive as to what to do when anomalies are revealed. Courts have been reluctant to dismiss election results, even in the extreme, such as when over 80% of the precinct ballot counts differ from the number of signatures in the polling books and the vendor has admitted to deploying an uncertified configuration of voting system components in violation of State requirements (ref. the 2006 Franklin County, Ohio recount case of Carole R. Squire vs. Christopher J. Geer).

In these matters, it generally falls to the contestor to prove that anomalies affected the results in such extent that, had they not occurred, the outcome would have been different. And the contestor must make this proof in the absence of access to the voting equipment or test results, since vendors and ITAs are allowed to claim trade secrecy protection for their materials. The 2007 draft VVSG further perpetuates this trade secrecy loophole (as had prior versions of the guidelines) by continuing to exempt COTS (commercial-off-the-shelf) products (including those with critical underpinnings such as device drivers and operating systems) from source code inspection and other standard reviews. This lax and dangerous view of COTS products is most evident in the fact that these are never required to be updated, even when new versions are issued to remedy known security risks.

One might think that, at least, if a voting system (or any of its components or modules) was found to be defective, or if the testing was discovered to have been improperly performed or deemed inadequate, there would be some process whereby the EAC would be required to withdraw certification. But the 2007 draft VVSG (like its predecessors) omits mention of any methodology whereby certification can be rescinded because of later-discovered flaws. The VVSG thus provides no protection to either the purchasers or the voters, since perversely, there is a disincentive for vendors to issue corrections to deployed systems, because any changes (even necessary ones) require costly recertification. The Catch-22 scenario is that you can continue to use defective voting machines, but you may not be able to obtain versions that have had the defect corrected. This situation must stop.

Most of the above issues are well-known and have been reported to the EAC in its various incarnations, by many people (including myself and Brad Friedman), numerous times. The 2007 draft VVSG continues the tradition of providing a set of straw hurdles that must be jumped over (or skirted around) in order to attain certification, while resulting in no true assurances. Another VVSG rewrite, novel designs, or more extensive testing cannot begin to solve these problems until the voters' demands for transparency, reliability, security, accuracy and auditability requirements have first been appropriately defined and addressed. So long as the goal of certification trumps the need to ensure election integrity, the resulting systems, no matter whose imprimatur they bear, will be invalid and must be rejected.



Uncommon Criteria

The software development process can benefit from the use of established standards and procedures to assess compliance with specified objectives, and reduce the risk of undesired behaviors. One such international standard for information security evaluation is the Common Criteria (CC, ISO IS 15408, csrc.nist.gov/cc). Although use of the CC is currently mandated in the U.S. for government equipment (typically military-related) that processes sensitive information whose "loss, misuse, or unauthorized access to or modification could adversely affect the national interest or the conduct of Federal programs" (Congressional Computer Security Act of 1987), it has been voluntarily applied in other settings (such as health care). In the U.S., oversight of CC product certification is provided by the National Institute of Standards and Technologies (NIST).

The goal of the CC is to provide security assurances via anticipation and elimination of vulnerabilities in the requirements, construction, and operation of IT products through testing, design review, and implementation. Assurance is expressed by degrees, as defined by selection of one of seven Evaluation Assurance Levels (EALs), and derived by assessment of correct implementation of the security functions appropriate to the level selected, and evaluation in order to obtain confidence in their effectiveness.

However, the use of standards is not a panacea because product specifications may contain simultaneously unresolvable requirements. Even the CC, regarded as a state-of-the-art standard, disclaims its own comprehensiveness, saying it is "not meant to be a definitive answer to all the problems of IT security. Rather, the CC offers a set of well-understood security functional requirements that can be used to create trusted products or systems reflecting the needs of the market." The CC methodology falls short in addressing and detecting potential design conflicts.

This major flaw of the CC is directly related to its security functional requirement hierarchy. In selecting an EAL appropriate to the product under evaluation, the CC specifies numerous dependencies among the items necessary for implementing a level's criteria of assurance. In essence, it formulates a mapping whereby if you implement X, you are required to implement Y (and perhaps also Z, and so on). But the CC fails to include a similar mapping for counterindications, and does not show that if you implement J then you cannot implement K (and perhaps also not L, and so on).

A good example of how this becomes problematic arises when both anonymity and auditability are required. The archetypical application of such simultaneous needs occurs in off-site election balloting, but one can also find this in such arenas as Swiss-style banking or AIDS test reporting. If the CC process were used with voting (no standards have been mandated, but NIST involvement is now being considered), it must assure that each ballot is cast anonymously, unlinkably, and unobservably, protecting the voter's identity from association with the voting selections. Because access to the ballot-casting modules requires prior authentication and authorization, pseudonymity through the use of issued passcodes provides a plausible solution. But the CC does not indicate how it is possible to maintain privacy while also resolving the additional requirement that all aliases must be traceable back to the individual voters in order to assure validity.

Furthermore, the need for anonymity precludes the use of traditional transaction logging methods for providing access assurances. Randomized audit logs have been proposed by some voting system vendors, but equipment or software malfunction, errors, or corruption can easily render these self-generated trails useless. Multiple electronic backups provide no additional assurances; if the error occurs between the point of user data entry and the writing of the cast ballot, all trails would contain the same erroneous information. Pure anonymity and unlinkability, then, are possible only if authentication and authorization transactions occur separately from balloting, but this is difficult to achieve in a fully electronic implementation.

The remedy to this and other such flaws in the CC involves augmentation with extensions that go beyond the current standard. For voting, one solution is to produce voter-verified paper ballots for use in recounts. Thus, the use of the CC in the secure product development cycle is encouraged, but prudent application and consideration of risks imposed by conflicting requirements is also necessary.

MARTIN MAYO

REBECCA MERCURI (mercuri@acm.org) is an assistant professor of CS at Bryn Mawr College; www.notablesoftware.com/evote.html.

Right Now

The expanding Harvard universe

BOLLIXED BALLOTS

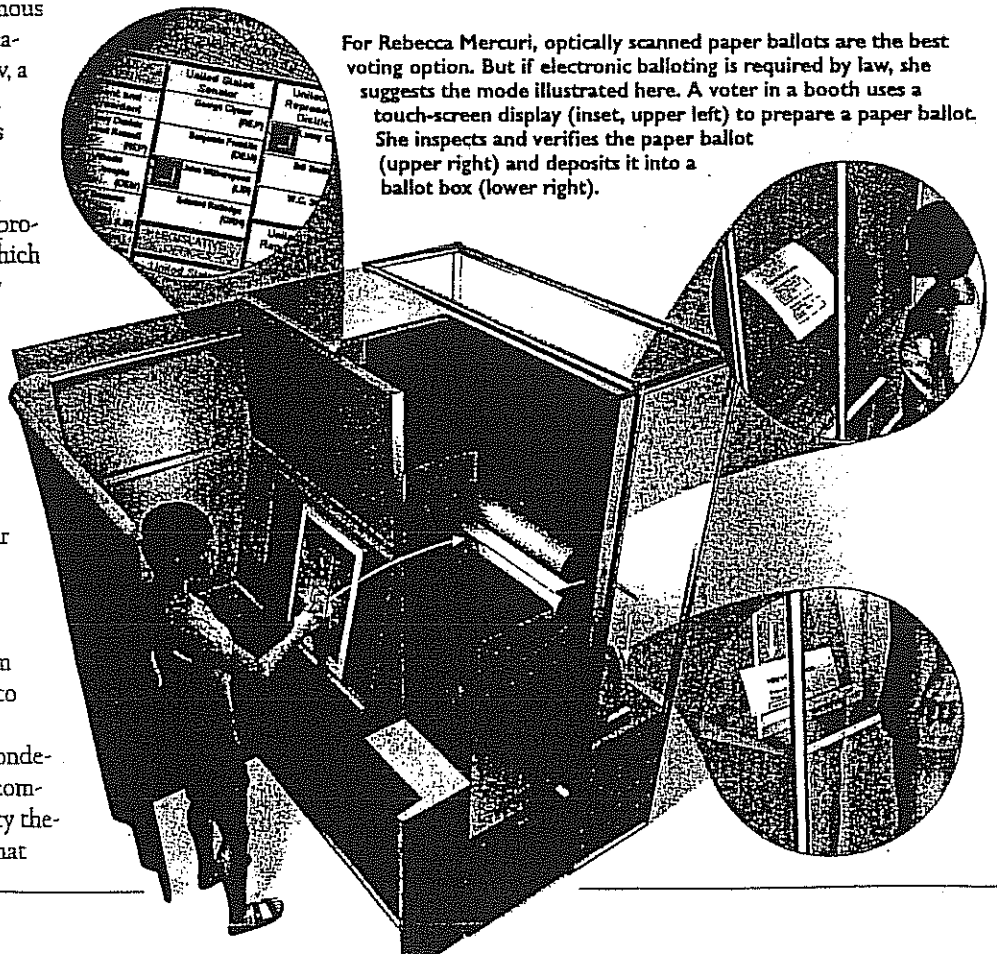
Voting into Vapor

FULLY ELECTRONIC SYSTEMS will record about one-third of the votes cast this November. But "Until and unless everyone understands NP-completeness and cryptographic theory," computer-security expert Rebecca Mercuri is "adamantly opposed to the use of any fully electronic or Internet-based systems for use in anonymous balloting and vote tabulation applications." The Radcliffe Institute fellow, a computer scientist who has studied electronic voting since 1989, believes that it is "incumbent upon all concerned with elections to *refrain* from procuring *any* system that does not provide an indisputable paper ballot which can be checked by the voter visually before deposit and used by the election board in case of a recount."

In a 2002 article in *IEEE* [Institute of Electrical and Electronics Engineers] *Spectrum* and many more recent publications, Mercuri argues that electronic voting is problematic in three ways: computer security, auditability, and transparency. All of these, she says, may pose insoluble difficulties.

The computer-security issues stem from a class of conundrums known to logicians and computer scientists as "NP-complete." ("NP" stands for "nondeterministic polynomial-time.") NP-complete problems are part of complexity theory, an aspect of computer science that deals with the resources needed to solve problems, if solving them is indeed feasible at all. Computers cannot solve NP-complete problems, except, theoretically, over an infinitely long time. Take, for example, the problem of optimizing a stock portfolio. "If computers could solve this problem, we'd all be very wealthy!" says Mercuri, with a laugh. "But computers can only approximate an answer. The problem with voting is that we need a non-approximate answer."

In an electronic election, an NP-complete problem arises when one asks if the computer software has been properly constructed to register and tabulate votes. "Can we *prove* that?" asks Mercuri. "If we could prove that computers had no viruses, then the machines could test themselves. But the fact is that computer scientists have not figured out a way to



For Rebecca Mercuri, optically scanned paper ballots are the best voting option. But if electronic balloting is required by law, she suggests the mode illustrated here. A voter in a booth uses a touch-screen display (inset, upper left) to prepare a paper ballot. She inspects and verifies the paper ballot (upper right) and deposits it into a ballot box (lower right).

ILLUSTRATION BY BRYAN CHRISTIE

prove that the software is perfect: doing only what we want and nothing else. We *could* do it if we had infinite time and every possible input and output, but the permutations quickly become astronomical. And if you change one line of code in the software, you have to run the test again."

Voting by secret ballot also conflicts with the need for auditability. "The way we audit something like banking or healthcare precludes anonymity, since we have to track each individual transaction, end-to-end," Mercuri explains. "But anonymous voting requires privacy, so we shut off this kind of tracking during the most critical part of the process: the balloting. With this [fully electronic] equipment, you cannot perform an independent recount. It's like asking Enron to give you a printout of their accounting data." (Only one state, Nevada, requires electronic polls to be accessible to audit via voter-verified paper ballots. "Ironic, but it makes sense," Mercuri explains. "They have to audit all these casino gaming machines, so they know how to audit computers.")

Third, says Mercuri, electronic voting "is still not sufficiently transparent for citizens of a democracy to have confidence in the system." Since computer voting involves advanced technology and complex software, "it provides an opportunity for an intellectual elite to control the system. Do you want cryptographers in control of the electoral process?"

Even so, electronic balloting is going ahead. The 2002 Help America Vote Act authorized $3.8 billion in spending though 2006; $3 billion of that is going to voting-systems vendors. Non-auditable, fully electronic voting technology will record 30 percent of 2004 presidential votes. Optically scanned paper ballots will tally another 50 percent, and mixed systems like lever machines and punch cards will record the remaining 20 percent. The balloting business is so concentrated, reports Mercuri, that two companies founded by two brothers will ultimately tabulate 80 percent of all votes cast.

"The equipment is extraordinarily expensive—small counties are paying as much as $25 million for electronic voting machines—and frankly, unnecessary," she asserts. "These machines are only used a couple of times a year, and the rest of the time have to sit in dark, air-conditioned warehouses. Their batteries run down and need replacement. Furthermore, people are now buying obsolete machines, since the money from the Help America Vote Act wasn't tied together with technical standards. I don't see that you'll be getting much bang for your buck."

The difficulties of electronic voting reappear even more clearly in on-line Internet voting, a novelty in which France, Germany, Australia, and Estonia have announced initiatives. On-line voting poses severe problems of voter identification, as

Right Now

well as offering vast potential for disruption by spoofing and denial-of-service attacks. "A secure Internet voting system is theoretically possible," wrote cryptographer Bruce Schneier, founder of Counterpane Internet Security, "but it would be the first secure networked application ever created in the history of computers."

Mercuri worries, too, about the expanded scale of potential abuses. "Whereas earlier technologies required that election fraud be perpetrated at one polling place or machine at a time," she wrote in her *IEEE Spectrum* piece, "the proliferation of similarly programmed e-voting systems invites opportunities for large-scale manipulation of elections." She closed with a comment from an unnamed observer of voting technology: "'If you think technology can solve our voting problems,' he said, 'then you don't understand the problems and you don't understand the technology.'"

—CRAIG LAMBERT

REBECCA MERCURI WEBSITE:
www.notablesoftware.com/evote.html

REBECCA MERCURI, PH.D. mercuri@acm.org
215/327-7105
RADCLIFFE INSTITUTE FOR ADVANCED STUDY
HARVARD UNIVERSITY

Un(der)addressed Issues in Voting System Standards

presented at the
First Open Workshop on the "Voluntary Voting System Guidelines"
Washington D.C., December 6, 2007
by

Rebecca Mercuri, Ph.D.
notable@notablesoftware.com
609/587-1886

There are numerous unaddressed and/or underaddressed issues or "gaps" in the existing and draft voting system standards and guidelines. The reasons for such gaps are manyfold and may stem from: misunderstandings regarding technology, procedures and policies and how these interact in voting systems; the desire to accommodate diverse special interest groups and election equipment stakeholders; a general orientation toward legacy balloting designs; inability to reconcile constraints that are mutually unsatisfiable; etc. Although an understanding of the causes of these gaps may assist in their resolution, that is left for later elaboration. This presentation enumerates some of the un(der)addressed issues I feel present primary concern in the establishment of effective and comprehensive voting system standards, toward the end of ensuring that these (and others identified as salient) will not continue to be ignored or dismissed.

- Form versus Function: Predisposition to existing metaphors and designs can "lock-out" new methodologies and features that cannot conform to or be validated by the prescribed structure, yet a purely functional definition of voting aspects may be infeasible or insufficiently detailed.
- COTS exemptions, Closed Source, Trade Secrecy: Identification of potential adverse impacts, mitigated with needs for concealment and inadequacies of escrow.
- Open Source and Components: Risks of compromise vs. benefits and feasibility of review.
- Object Code: Signatures validate instantiation, not correctness.
- Transparency, Checks & Balances: System and process, end-to-end vs. critical points.
- Software Independence: Socio-technological assessment to determine software involvement.
- Common Criteria Protection Profile: Structure for methodically addressing security and risks.
- Mutually Unsatisfiable Constraints: Conflicting requirements of the voting process (such as full anonymity with full auditability) identified and mitigation approaches suggested.
- Logical Provability: Feasibility of determination of correctness for design and implementation of math-critical modules (such as with cryptography, randomization, rank and tiered count methods, etc.).
- Reliability and Accuracy: Methods for assessment system-wide, components and modules.
- Modularization: Impacts of interaction between and among modules.
- External Processes: Ballot definition, pollbooks, tabulation and count aggregation, document handling procedures, equipment transportation, etc., relationships and effects, best practices.
- Pre- and Post-Election Testing: Relevance and assurances of correct operation, functionality.
- Auditability and Verification: Independence, redundancies, comprehensivity, circumvention.
- Certification: Testing authorities, privatization, fees, federal/state/local differences.
- Error Reports and Updates: Collection, dissemination, evaluation.
- Decertification and Recall: Systems, modules, components.

"The Way Democracy Will Be"

6930 Carroll Ave., Suite 610
Takoma Park, MD 20912 - (301) 270-4616
(301) 270-4133 (fax) · info@fairvote.org
www.fairvote.org

Rob Richie
Executive Director, FairVote

Written Testimony Submitted to EAC
Re: 2007 Voluntary Voting System Guidelines
April 21st, 2008

As Executive Director of FairVote, a non-partisan, not for profit organization, I thank you for the opportunity to submit written testimony on the August 2007 Technical Guidelines Development Committee's (TGDC) Recommendations for the Voluntary Voting System Guidelines (VVSG). Serving as a catalyst for reform, FairVote has been proactive in transforming our elections to reflect the will of the people by translating votes into fair representation. In particular, we believe ranked choice voting systems such as choice voting for multi-seat districts used in Cambridge [MA] and instant runoff voting (IRV) for single seat elections, used or will soon be implemented in Minneapolis [MN], Oakland [CA], Pierce County [WA] and San Francisco [CA], create election results that most closely embody the democratic principles of majority rule and equal representation.

In regards to the discussion questions advanced by the EAC in anticipation of the April 24th Voting Advocates Roundtable Discussion, this testimony will directly address question two on innovative systems and question six regarding potential changes to the VVSG. While FairVote strongly supports election security and integrity of the vote (as outlined in question one), I will defer to other advocates and experts on the many particulars about how best to achieve it. I have attached FairVote's position statement on this matter in the appendix for your reference. We believe the EAC plays a vital role in ensuring municipalities can effectively administer elections including those with ranked voting systems and the VVSG should provide sufficient guidance to election system manufacturers to develop equipment to accommodate such systems that are also secure, reliable, easy to use and accessible to all voters.

As the EAC develops the VVSG, please consider the following comments to the roundtable discussion questions and supplements in the appendix.

Systems Innovation

The current lengthy and costly VVSG certification process does not foster innovation and stymies creativity in developing new voting systems. Additionally, certification of advancements and minor technical adjustments often require a lengthy re-certified process, prompting manufacturers to attempt to hide rather than correct minor glitches and also prevent manufacturers from providing additional features to current systems requested by election officials. FairVote urges the creation of two new categories of expedited certification in addition to the innovation systems envisioned in

the proposal. These two new categories should have evaluation and certification that is even simpler and quicker than regular innovation systems to be included in the VVSG.

These two new categories subject to a super-streamlined process may be named "highly transparent innovation systems" and "minor modifications to certified systems."

A system would be considered "highly transparent" if the system meets these criteria:

> 1. The system has a clear and non-controversial audit method that allows for re-tallying elections using the original voter inputs (such as hand-counting from marks on paper ballots);
>
> 2. The system uses exclusively COTS electronic hardware and either COTS or open-source software that can be widely, if informally, "tested" by "outsiders."

For example, among private associations, some elections are conducted using cheaply-printed paper ballots with COTS scanners, COTS mark-sense software and COTS spreadsheets for tallying. Perhaps such a method could be used for all mail elections or in conjunction with a certified ballot marking system like the AutoMark for disability voting. The existence of both scanned images and paper ballots allow for easy and even redundant auditing. Such an innovative approach could arguably be described as not even a "voting system" subject to certification under VVSG at all, but any lack of clarity on that point could prevent its utilization in a state piggybacking on the VVSG.

Changes to existing systems that do not substantially alter the already certified voting equipment, may be deemed "minor modifications to certified systems," and subject to the super-streamlined and low cost certification process. Currently, voting system guidelines are not comprehensive and do not accommodate nor reflect election system reforms currently being implemented by states. For example, modifications of voting systems to include ranked choice voting should be considered in this classification since such technical adjustments do not necessarily interfere with the integrity of existing voting systems.

In the past, the failure of leadership by election administrators and voting equipment manufacturers to prepare for ranked choice voting has caused severe strains and costs on communities. For example, San Francisco was forced to violate its charter because the city failed to use instant runoff voting in its 2003 mayoral elections. San Francisco was able to avoid a lawsuit simply because the judge admitted he could not force the jurisdiction to run elections it was not prepared to do, largely in part due to the vendor being ill-equipped for handling ranked voting elections. Similarly, cities such as Ferndale [MI], Berkeley [CA], Sarasota [FL] and Oakland [CA] faced non-compliance with local legislation mandating IRV due to the lack of certified voting technology capable of running such elections. Other jurisdictions, Takoma Park [MD] and Cary [NC], have had to work around current technology to implement IRV with the first employing paper ballots and the later developing an innovative method of counting first choice votes on voting machines in polling sites with subsequent IRV rounds tallied by hand at the precinct level. The “Instant Runoff Voting Procedures” for Cary [NC] are included in the appendix for your reference.

Amendments to VVSG

As illustrated, current VVSG are not comprehensive and does not provide sufficient guidance for jurisdictions to adjust to changes in election systems. Instead, what is included as standards are often piecemeal in nature and reactionary in practice. As other jurisdictions like Burlington [VT] consider alternative voting systems such as ranked choice voting, FairVote urges the EAC to develop and include clear guidelines in the VVSG to assist local election administrators and voting system manufacturers. As an example, the Minnesota Secretary of State, Mark Ritchie, has created an advisory committee to establish standards for how to run ranked voting elections. The recommendations have been adopted and introduced as state legislation (HF 3006 and SF 3247), see appendix. Additionally, we have included in the appendix *Ranked Voting Guidelines*, a draft voting system standard that could serve as an example for what guidelines could look like (FairVote and the ranked choice voting community have not endorsed any/all parts of the document). We look forward to working with the EAC to create a working group or taskforce to develop much-needed standards for ranked choice voting technology.

Other changes we recommend to the VVSG are more technical in nature, and we have included these amendments in the appendix. Thank you for the opportunity to submit this testimony, which was written with the assistance of Terrill Bouricius, David Moon and Amy Ngai. I look forward to further exploring some of these issues introduced here in the roundtable discussion on Thursday.

Appendix I: FairVote Position on Voting Equipment, Election Integrity & Auditability
Appendix II: Instant Runoff Voting Procedures, Town of Cary
Appendix III: Minnesota Legislation HF 3006 & SF 3247
Appendix IV: *Ranked Voting Guidelines*
Appendix V: FairVote Comments on TGDC's VVSG

Appendix I

FairVote Position on Voting Equipment, Election Integrity & Auditability

Any voting technology used for government elections in the U.S. should be secure, accurate, reliable and auditable. To ensure confidence in elections and to provide a paper record, voting machines should use a voter-verified paper ballot that is the basis for recounts and auditing the election. Direct recording equipment (DRE's) should be replaced with paper-based voting methods such as Optical Scan and AutoMark-type technology that utilizes a genuine paper ballot. The ideal method, to maximize security and integrity, is to have a redundant record of every vote. This means a system that has both a computerized record, or "ballot image" of each vote, as well as a paper ballot record of each individual vote (rather than merely running totals). This allows the comparison of the two records as an additional layer of security.

Optical scan machines are examples of acceptable technology. Paper ballot machines with a computerized interface may be acceptable if they generate paper ballots as the official ballots of record and print ballots that are easily readable and test well for usability.

These should be coupled with a manual audit and other protocols such as proper pre- and post-election testing, ballot accounting and secure chain of custody. All government elections should be subject to random, manual, statistical audits able to confirm election outcomes with a high level of confidence. Because Internet voting cannot achieve the standards above, it should not be used for government elections in the U.S. We recognize the right of private associations to run their election on-line if their members are willing to accept the inherent risk that comes with online voting.

Advanced voting methods, such as those using ranked-choice ballots, pose no more risk of fraud than more commonly used voting methods and do not depend on the use of electronic voting. FairVote urges jurisdictions, whether adopting advanced voting methods or not, to also institute the above recommended procedures and voter-verifiable and auditable voting technologies. We urge jurisdictions to set a new and higher standard of transparency by following the precedent of cities such as Burlington, VT and San Francisco, CA, in running ranked-ballot elections, and implement "open source ballots" by also posting the computerized record of every ballot on the Internet.

Longer term, FairVote believes that voting equipment and election administration in the United States requires a national elections commission to create minimum national election standards, and explore purchase of "public interest voting equipment" whereby the software and voting equipment is open source and publicly owned.

INSTANT RUNOFF VOTING PROCEDURES
TOWN OF CARY
OCTOBER 9, 2007 ELECTION

- There are 36 precincts in the Town of Cary

- The majority of the precincts will have more than one ballot style depending on the Board of Education District, outside municipal jurisdiction, etc. The following are ballots for the Town of Cary:
    1. Town of Cary/County Bond
    2. Town of Cary/Board of Education/County Bond
    3. Board of Education/County Bond
    4. County Bond
    5. One precinct will also have a City of Raleigh ballot

- As the sealed voted ballot boxes are returned to the Board of Elections office, Cary precincts will be set aside and the voted precincts returned to the Conference Room. The lock on the conference room will be changed prior to Election Day. Security guards are posted outside the conference room.

- As the sealed provisional ballot bags are returned to the Board of Elections office, Cary precincts will immediately be brought to G-8 of the Board of Elections to begin the audit of the number of provisional ballots per precinct. This will give us an approximate number of provisional ballots cast in the Town of Cary election – but not an exact number of what the Board will approve to be counted.

- Notice will be given that the Board will meet for the sample audit after which time, the Board will discuss the count of the IRV.

- When the Board meets on Thursday, October 11th to conduct the sample audit, a review of the unofficial results and the number of provisional ballots cast will be a good indicator if any candidate in any particular race received majority vote or if the IRV will take effect.

- Once the Board determines that no candidate in a particular race would reach majority, the Board will divide into teams for the 2nd and 3rd choice vote counts.

- The Board will divide into 3 separate teams – one Board Member and two officials to tally the votes.

- All counting will be done in the secure Wake County Office Building Conference Room. Projectors will be set up for all observers to be able to see the ballots being sorted and hand counted. *

*In accordance with NCGS 163-165.1(e), "Any person who has access to an official voted ballot or record and knowingly discloses in violation of this section how an individual has voted that ballot is guilty of a Class 1 Misdemeanor."

SORTING PROCEDURES FOR EACH CONTEST INDIVIDUALLY

Team 1

Box of Sealed Voted Ballots

Team Members
- 1 Board Member
- 2 Officials

Task
- Sort
- Tally

Team 2

Box of Sealed Voted Ballots

Team Members
- 1 Board Member
- 2 Officials

Task
- Sort
- Tally

Team 3

Box of Sealed Voted Ballots

Team Members
- 1 Board Member
- 2 Officials

Task
- Sort
- Tally

Step-by-Step Procedures

At any time a Board Member cannot determine the voter's intent on a particular ballot, the entire Board will meet to review the ballot and vote to determine the voter's intent, if at all possible.

STEP 1 - Sort

1. Board member will unseal box of ballots, identifying the precinct number and the ballot styles contained in the ballot box.

2. Sort ballots.

    - If more than one ballot style in a precinct, the non-Cary ballots will be placed in a separate stack (Stack #3).
    - First sort will be 2 stacks – 3 stacks if non-Cary ballots in the precinct
    - As a result of the Election Night Returns (to include Absentee by Mail, One-Stop Absentee Early Voting, Provisional, and Transfer Site), the candidates for each contest that received the most votes will be identified. Each candidate will be referred to in this document as "Candidate A" and "Candidate B".

3. A Board Member reviews each ballot. The Member will state whether there is a vote in Column 1 for Candidate A or Candidate B. Ballots will be placed in one of 3 stacks. (Stack #1, Stack #2, or Stack #3)

    - STACK #1 - If the ballot does contain a vote for Candidate A or Candidate B in Column 1, the ballot is placed in Stack #1. (This ballot will not be tallied)
    - STACK #2 - If the ballot does not contain a vote in Column 1 for Candidate A or Candidate B, the ballot is placed in Stack #2.
    - STACK #3 - If the ballot is a non-Cary ballot, the Board Member will state non-Cary ballot and place the ballot in stack #3. (This ballot will not be tallied)

STEP 2 - Column 2 Tally

Once all ballots for one precinct have been sorted, the hand count of Column 2 will begin. (Stack #2)

4. The Board Member will ONLY review Column 2 on each ballot and state if there is a vote for Candidate A or Candidate B. If so, the vote will be tallied. After the ballot is tallied, the ballot will be turned over to signify that the ballot has now been tallied and be placed in Stack #2A.

    - While the Board Member begins to review Column 2, a separate "official" will verify that the ballots sorted into Stack #1 and Stack #3 was properly conducted.
    - Any ballots not properly sorted are brought to the attention of the Board Member and the sort team for placement into the correct stack.

5. If there is no vote in Column 2 for Candidate A or Candidate B, the ballot will be placed in Stack #2B for Column 3 ballots.

STEP 3 - Column 3 Tally

6. After all ballots have been tallied for Column 2, the Board Member will review Column 3 in Stack #2B. The Member will state if there is a vote for Candidate A or Candidate B. If so, the vote will be tallied. The ballot will be turned over and placed in Stack #2C to signify that the ballot has now been tallied.

7. If there is no vote in Column 3 for Candidate A or Candidate B, the ballot will be placed in Stack #2D for ballots with no Candidate A or B choices.

8. Once all votes have been tallied for Candidate A or Candidate B, the hand count totals will be added to the Official Results for that Contest.

9. All ballots from the counted precinct will be returned to the original ballot box and sealed until the next contest needs to be counted, if any.

10. Precinct ballot from the counted precincts will be placed in a separate location to indicate the precinct ballots have been counted.


Unseal Box Cary Precinct Ballot Box
Sort Ballots / Review Ballots
Stack #1 Vote For Candidate A or B in Column 1
Stack #2 No Vote For Canidate A or B in Column 1
Stack #3 Non-Cary Ballots
Do Not Tally
Review Column #2
Do Not Tally
Is Vote for Canidate A or B? (In Column #2)
Yes
No
Tally Vote for Candidates A or B Column #2 Only
Place Ballot in Stack #2B
Turn Ballot Over Place in Stack #2A
ONLY AFTER All Ballots in Stack #2 have been processed, proceed to the next step.
Is Vote For Candidate A or B? (In Column #3)
Yes
No
Tally Vote for Candidate A or B Column #3 Only
Place Ballot In Stack #2D
Turn Ballot Over Place #2C

A bill for an act

relating to elections; establishing procedures for home rule charter jurisdictions that adopt ranked-choice voting; amending Minnesota Statutes 2006, sections 205.13, subdivision 2; 206.83; proposing coding for new law in Minnesota Statutes, chapter 206; proposing coding for new law as Minnesota Statutes, chapter 204E.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF MINNESOTA:

Section 1. **[204E.01] APPLICABILITY.**

(a) This chapter applies to all elections conducted using ranked-choice voting. All other provisions of Minnesota Statutes also apply, to the extent they are not inconsistent with this chapter.

(b) Except as otherwise provided, a jurisdiction that chooses to adopt ranked-choice voting pursuant to section 204E.03 must conduct the elections according to the method and procedures established by this chapter.

Sec. 2. **[204E.02] DEFINITIONS.**

Subdivision 1. **Scope.** The definitions in this section apply to this chapter.

Subd. 2. **Batch elimination.** "Batch elimination" means a simultaneous defeat of multiple continuing candidates that have no mathematical chance of being elected.

Subd. 3. **Continuing candidate.** "Continuing candidate" means a candidate who has been neither elected nor defeated.

Subd. 4. **Defective ballot.** "Defective ballot" means a ballot in which a first ranking is not indicated or if more than one candidate is given a first ranking.

Subd. 5. **Duplicate ranking.** "Duplicate ranking" occurs when a voter ranks the same candidate at multiple rankings.

Subd. 6. **Exhausted ballot.** "Exhausted ballot" means a ballot that cannot be transferred to a lower ranked candidate because the next ranking is blank or there is more than one candidate given the next ranking.

Subd. 7. **Highest continuing ranking.** "Highest continuing ranking" means the ranking on a voter's ballot with the lowest numerical value for a continuing candidate.

Subd. 8. **Overvote.** An "overvote" occurs when a voter ranks more than one candidate at the same ranking.

Subd. 9. **Ranked-choice voting.** "Ranked-choice voting" means an election method in which voters rank candidates for an office in order of their preference and the ballots are counted in rounds that, in the case of a single-seat election, simulate a series of runoffs until one candidate meets the threshold, or until two candidates remain and the candidate with the greatest number of votes is declared elected. In the case of multiple-seat elections, the series of runoffs are simulated until all seats to be elected have been filled.

Subd. 10. **Ranked-choice voting tabulation center.** "Ranked-choice voting tabulation center" means the place selected for the automatic or manual processing and tabulation of ballots.

Subd. 11. **Ranking.** "Ranking" means the number assigned by a voter to a candidate to express the voter's preference for that candidate. Ranking number one is the highest ranking. A ranking of lower numerical value indicates a greater preference for a candidate than a ranking of higher numerical value.

Subd. 12. **Round.** "Round" means an instance of the sequence of voting tabulation steps established in sections 204E.06 and 204E.07.

Subd. 13. **Skipped ranking.** "Skipped ranking" occurs when a voter leaves a ranking blank and ranks a candidate at a subsequent ranking.

Subd. 14. **Surplus.** "Surplus" means the total number of votes cast for an elected candidate in excess of the threshold.

Subd. 15. **Surplus fraction of a vote.** "Surplus fraction of a vote" means the surplus divided by the total votes cast for the elected candidate, calculated to four decimal places. Surplus fraction of a vote = (Surplus)/(Total votes cast for elected candidate).

Subd. 16. **Threshold.** "Threshold" means the number of votes sufficient for a candidate to be elected. In any given election, the threshold equals the total votes counted in the first round after removing defective ballots, divided by the sum of one plus the number of offices to be filled and adding one to the quotient, disregarding any fractions. Threshold = (Total votes cast)/(Seats to be elected + 1) +1.

Subd. 17. **Transferable vote.** "Transferable vote" means a vote or a fraction of a vote for a candidate who has been either elected or defeated.

Subd. 18. **Undervote.** An "undervote" occurs when a voter does not rank any candidates for an office.

Sec. 3. **[204E.03] IMPLEMENTATION OF RANKED-CHOICE VOTING.**

(a) A home rule charter city or county that adopts the use of ranked-choice voting in local elections must adopt a charter amendment no later than 30 days before the first day for filing affidavits of candidacy for the office for which ranked-choice voting is to be used as the method of election.

(b) The use of ranked-choice voting may be eliminated through repeal of the charter amendment no later than 30 days before the first day for filing affidavits of candidacy for offices for which ranked-choice voting is used as the method of election.

(c) The chief election official in the jurisdiction must notify the secretary of state and, if applicable, the county auditor within 30 days following adoption or repeal of the charter amendment.

Sec. 4. **[204E.04] BALLOTS.**

Subdivision 1. **Ballot format.** (a) A ballot must allow a voter to rank at least three candidates for each office in order of preference and must also allow the voter to add write-in candidates.

(b) A jurisdiction may use ballots compatible with alphanumeric character recognition voting equipment.

Subd. 2. **Mixed-election method ballots.** If elections are held in which ranked-choice voting is used in addition to other methods of voting, the ranked-choice voting and non-ranked-choice voting elections must be on the same ballot card if possible, with ranked-choice voting and non-ranked-choice voting portions clearly separated on the ballot card. A separate ballot card may be used if necessary. A jurisdiction may deviate from the standard ballot order of offices to allow separation of ranked-choice voting and non-ranked-choice voting elections.

Subd. 3. **Ballot instructions.** (a) In an election held using optical-scan voting technology, the ballot must include instructions to voters appearing substantially as follows:

"INSTRUCTIONS: Mark your first choice in the first column by completely filling in the oval next to your choice, as shown in the picture. To indicate a second choice, select a different candidate in the second column. To indicate a third choice, select a different candidate in the third column.

1. Rank candidates in order of your preference.

2. You may rank as few candidates as you wish or as many as is allowed.

3. Do not skip rankings.

4. Do not give the same ranking to more than one candidate.

5. Do not rank the same candidate more than once."

(b) In an election held using alphanumeric character recognition technology, the ballot must contain the instructions as provided in paragraph (a), provided that the instructions may be modified where necessary to reflect the appearance and layout of the ballot.

Sec. 5. **[204E.05] RANKED-CHOICE VOTING TABULATION CENTER.**

The chief election official in the jurisdiction shall designate one location to serve as the ranked-choice voting tabulation center. The center must be accessible to the public for the purpose of observing the vote tabulation. Tabulation of votes must be conducted as described in sections 204E.06 and 204E.07.

Sec. 6. **[204E.06] TABULATION OF VOTES; SINGLE-SEAT ELECTIONS.**

Subdivision 1. **Applicability.** This section applies to a ranked-choice voting election in which one seat in office is to be filled from a single set of candidates on the ballot. The method of tabulating ranked-choice votes for single-seat elections as described in this section must be known as the "single-seat single transferable vote" method of tabulation.

Subd. 2. **Precinct tabulation.** When the hours for voting have ended and all voting has concluded, the election judges in each precinct shall record and publicly declare the number of votes at each ranking on the ballot. The election judges must then securely transfer all electronic voting data, if applicable, from the precinct to the ranked-choice voting tabulation center designated pursuant to section 204E.05.

Subd. 3. **Ranked-choice voting tabulation center.** (a) Tabulation of votes at the ranked-choice voting tabulation center must proceed in rounds. First the threshold must be calculated and publicly declared. After calculation of the threshold, each round must proceed sequentially as follows:

(1) The number of votes cast for each candidate, as indicated by the highest continuing ranking on each ballot, must be counted. If a candidate's vote total is equal to or greater than the threshold, the tabulation is complete. If no candidate's vote total is equal to or greater than the threshold, the tabulation must continue as described in clause (2).

(2) Candidates appearing on the ballot who do not receive any votes are defeated immediately, before any transfers.

(3) All candidates are defeated whose vote total, plus all potentially transferable votes from candidates with fewer votes, is less than the vote total of the candidate with the next higher number of votes, such that it is mathematically impossible for that candidate to be elected. All candidates for whom it is mathematically impossible to be elected must be considered defeated simultaneously.

(4) The candidate with the fewest votes is defeated. Votes for the defeated candidate must be transferred to each ballot's next-ranked continuing candidate. Ties between candidates with the fewest votes must immediately and publicly be decided by lot by the chief election administrator at the tabulation center. The candidate chosen by lot must be defeated. The result of the tie resolution must be recorded and reused in the event of a recount.

(5) The procedures in clauses (1) to (4) must be repeated until one candidate reaches the threshold, or until only two continuing candidates remain. If only two candidates remain, the candidate with the most votes must be elected. In the case of a tie between two continuing candidates, the tie must be decided by lot as provided in section 204C.34. The result of the tie resolution must be recorded and reused in the event of a recount.

(b) If any ballot cannot be advanced because no further continuing candidates are ranked on that ballot, or because a voter has skipped a ranking or ranked the same candidate in two or more rankings, that ballot must immediately be declared "exhausted." Any ballot that has been declared an undervote, overvote, or exhausted must not count towards any candidate in that round or in subsequent rounds.

Sec. 7. **[204E.07] TABULATION OF VOTES; MULTIPLE-SEAT ELECTIONS.**

Subdivision 1. **Applicability.** This section applies to a ranked-choice voting election in which more than one seat in office is to be filled from a single set of candidates on the ballot. The method of tabulating ranked-choice votes for multiple-seat elections as described in this section must be known as the "multiple-seat single transferable vote" method of tabulation.

Subd. 2. **Precinct tabulation.** When the hours for voting have ended and all voting has concluded, the election judges in each precinct must record and publicly declare the number of votes at each ranking on the ballot. The election judges must then securely transfer all electronic voting data, if applicable, from the precinct to the ranked-choice voting tabulation center designated pursuant to section 204E.05.

Subd. 3. **Ranked-choice voting tabulation center.** (a) Tabulation of votes at the ranked-choice voting tabulation center must proceed in rounds. First the threshold must

be calculated and publicly declared. After calculation of the threshold, each round must proceed sequentially as follows:

(1) The number of votes cast for each candidate, as indicated by the highest ranked continuing candidate on each ballot, must be counted. If the number of candidates whose vote totals equal or exceed the threshold is equal to the number of seats to be filled, the tabulation is complete.

(2) Surplus votes for any candidates whose vote total is equal to or greater than the threshold must be calculated.

(3) Candidates appearing on the ballot who do not receive any votes are defeated immediately, before any transfers.

(4) After any surplus votes are calculated but not yet transferred, a candidate is defeated whose vote total, plus all potentially transferable votes from elected candidates and candidates with fewer votes, is less than the vote total of the candidate with the next higher number of votes, such that it is mathematically impossible for that candidate to be elected. All candidates for whom it is mathematically impossible to be elected must be defeated simultaneously.

(5) The surplus fraction of each vote cast for an elected candidate must be transferred to the next continuing candidate on that ballot. If two or more candidates have vote totals that equal or exceed the threshold, the surplus fraction of the votes cast for the elected candidate with the most votes must be transferred to the next continuing candidate on each ballot. The surplus fraction of votes cast for other elected candidates, in order of vote totals, must then be transferred to the next continuing candidate on each ballot. A tie between two or more candidates must immediately and publicly be resolved by lot by the chief election administrator at the tabulation center. The candidate chosen by lot must be defeated. The result of the tie resolution must be recorded and reused in the event of a recount.

(6) If there are no transferable surplus votes, the candidate with the fewest votes is defeated. Votes for the defeated candidate are transferred to each ballot's next-ranked continuing candidate. Ties between candidates with the fewest votes must be decided by lot, and the candidate chosen by lot must be defeated. The result of the tie resolution must be recorded and reused in the event of a recount.

(7) The procedures in clauses (1) to (6) must be repeated until the number of candidates whose vote totals equal or exceed the threshold is equal to the number of seats to be filled, or until the number of continuing candidates is equal to the number of offices yet to be elected. If the number of continuing candidates is equal to the number of offices yet to be elected, the remaining continuing candidate must be declared elected. In the case

of a tie between two continuing candidates, the tie must be decided by lot as provided in section 204C.34, and the candidate chosen by lot must be defeated. The result of the tie resolution must be recorded and repeated in the event of a recount.

(b) If any ballot cannot be advanced because no further candidates are ranked on that ballot, that ballot must immediately be declared "exhausted." Any ballot that has been declared an undervote, overvote, or exhausted must remain so and shall not count towards any candidate in that round or in subsequent rounds.

Subd. 4. **Alternate counting methods.** Notwithstanding subdivision 1, a jurisdiction may use a different ranked-choice counting method for multiple-winner elections upon application to and approval of the secretary of state. The secretary of state must adopt rules governing the approval of alternate counting method applications.

Sec. 8. **[204E.08] WRITE-IN PROCEDURES.**

In the event that votes cast for the write-in category are not eliminated as provided in section 204E.06, subdivision 2, or 204E.07, subdivision 3, each ballot must be examined by the elections administrator and the results must be entered into the ranked-choice voting tabulation software.

Sec. 9. **[204E.09] REPORTING RESULTS.**

(a) Each precinct must print a precinct summary statement, which must include the number of votes in each ranking for each candidate.

(b) The ranked-choice voting tabulation center must print a summary statement, which must include the following information: total votes cast; number of undervotes; number of defective and spoiled ballots; threshold calculation; total first choice rankings for all candidates; round-by-round tabulation results, including simultaneous batch eliminations, surplus transfers, and defeated candidate transfers; and exhausted ballots at each round.

(c) The election abstract must include the information required in the ranked-choice voting tabulation center summary statement, with the addition of the number of registered voters by precinct, the number of same day voter registrations, and the number of absentee voters.

Sec. 10. **[204E.12] RECOUNTS.**

(a) A candidate defeated in the final round of tabulation may request a recount as provided in section 204C.36.

(b) A candidate defeated in an earlier round of tabulation may request a recount at the candidate's own expense. The candidate is responsible for all expenses associated with the recount regardless of the vote difference between the candidates in the round in which the requesting candidate was defeated.

Sec. 11. **[204E.13] RULES.**

The secretary of state may adopt rules necessary to implement the requirements and procedures established by this chapter.

Sec. 12. Minnesota Statutes 2006, section 205.13, subdivision 2, is amended to read:

Subd. 2. **Notice of filing dates.** At least two weeks before the first day to file affidavits of candidacy, the municipal clerk shall publish a notice stating the first and last dates on which affidavits of candidacy may be filed in the clerk's office and the closing time for filing on the last day for filing. The clerk shall post a similar notice at least ten days before the first day to file affidavits of candidacy. The notice must indicate the method of election to be used for the offices on the ballot. If ranked-choice voting is to be used for a multiple-winner election and the method of tabulating votes is different from that described in section 204E.07, the notice must also indicate the date on which the secretary of state approved the alternate tabulation method and a location at which a full copy of the tabulation procedures to be used may be inspected.

Sec. 13. **[206.802] ELECTRONIC VOTING SYSTEMS; PURCHASING.**

Any new voting equipment purchased for use in Minnesota for the purpose of replacing a voting system must have the ability to:

(1) capture and store ballot data;

(2) keep data anonymous;

(3) accept ranked or cumulative voting data under a variety of tabulation rules;

(4) be programmable to follow all other specifications of the ranked-choice voting system as provided in chapter 204E;

(5) provide a minimum of three rankings for ranked-choice voting elections;

(6) notify voters of the following errors: overvotes, skipped rankings, and duplicate rankings in a ranked-choice voting election; and

(7) be programmable to print a zero tape indicating all rankings for all candidates in a ranked-choice voting election.

EFFECTIVE DATE. This section is effective upon certification by the secretary of state that equipment meeting the standards required by this section is available for purchase and implementation.

Sec. 14. Minnesota Statutes 2006, section 206.83, is amended to read:

206.83 TESTING OF VOTING SYSTEMS.

(a) Within 14 days before election day, the official in charge of elections shall have the voting system tested to ascertain that the system will correctly mark ballots using all methods supported by the system, including ranked-choice voting if applicable, and through assistive technology, and count the votes cast for all candidates and on all questions. Public notice of the time and place of the test must be given at least two days in advance by publication once in official newspapers. The test must be observed by at least two election judges, who are not of the same major political party, and must be open to representatives of the political parties, candidates, the press, and the public. The test must be conducted by (1) processing a preaudited group of ballots punched or marked to record a predetermined number of valid votes for each candidate and on each question, and must include for each office one or more ballot cards which have votes in excess of the number allowed by law in order to test the ability of the voting system tabulator and electronic ballot marker to reject those votes; and (2) processing an additional test deck of ballots marked using the electronic ballot marker for the precinct, including ballots marked using the electronic ballot display, audio ballot reader, and any assistive voting technology used with the electronic ballot marker. If an election is to be conducted using ranked-choice voting, the equipment must also be tested to ensure that each ranking for each candidate is recorded properly.

(b) If any error is detected, the cause must be ascertained and corrected and an errorless count must be made before the voting system may be used in the election.

(c) After the completion of the test, the programs used and ballot cards must be sealed, retained, and disposed of as provided for paper ballots.

Sec. 15. **[206.892] POSTELECTION AUDIT OF VOTING SYSTEMS; RANKED-CHOICE VOTING ELECTIONS.**

Subdivision 1. **Definition.** For purposes of this section, "postelection audit official" means the election administration official who is responsible for the conduct of elections in the jurisdiction being audited under this section.

Subd. 2. **Selection for audit; notice.** Thirty days before an election that will be conducted using the ranked-choice voting method pursuant to chapter 204E, the

postelection audit official must set the date, time, and place for postelection audit. Within four days after the election, the postelection audit official must select the precincts to be audited. Jurisdictions with fewer than 50,000 registered voters must select at least two precincts for postelection audit. Jurisdictions with between 50,000 and 100,000 registered voters must select at least three precincts to be audited. Jurisdictions with over 100,000 registered voters must select at least four precincts to be audited. The precincts must be selected by lot at a public meeting. At least one precinct selected in each county must have had more than 150 votes cast at the election. The postelection audit official must notify the secretary of state of the precincts that have been chosen for audit and the time and place the postelection audit for that jurisdiction will be conducted, as soon as the decisions are made. The secretary of state must post this information on the secretary of state's Web site.

Subd. 3. **Scope and conduct of audit.** The postelection audit must be conducted of the votes cast for at least one single-seat ranked-choice voting election, if applicable, and at least one multiple-seat ranked-choice voting election, if applicable. The audit must be conducted of elections decided most closely in the final round, by percentage. The postelection audit official may conduct a postelection audit of the votes cast for additional offices. The postelection audit must be conducted in public at the location where the voted ballots have been securely stored after the general election or at another location chosen by the postelection audit official. The postelection audit official for each precinct selected must conduct the postelection audit and may be assisted by election judges designated by the postelection audit official for this purpose. The party balance requirement of section 204B.19 applies to election judges designated for the audit. The postelection audit must consist of a manual count of the ballots used in the precincts selected and must be performed in the manner provided by section 204C.21. To the extent practicable, the postelection audit must be conducted in the manner provided for recounts under section 204C.361. The postelection audit must also include testing of the accumulation software, using stored electronic data for those precincts that are not audited by manual count. The audit must be completed no later than two days before the meeting of the canvassing board to certify the results of the election.

Subd. 4. **Standard of acceptable performance by voting system.** A comparison of the results compiled by the voting system with the postelection audit described in this section must show that the results of the electronic voting system differed by no more than one-half of one percent from the manual count of the offices audited. Valid votes that have been marked by the voter outside the vote targets or using a manual marking device that cannot be read by the voting system must not be included in making the determination whether the voting system has met the standard of acceptable performance for any precinct.

Subd. 5. **Additional review.** (a) If the postelection audit in one of the audited precincts reveals a difference greater than one-half of one percent or greater than two votes in a precinct where 400 or fewer voters cast ballots, the postelection audit official must, within two days, conduct an additional audit of the races indicated in subdivision 3 in at least three precincts in the same jurisdiction where the discrepancy was discovered. The postelection audit official must immediately publicly select by lot the additional precincts to be audited. The postelection audit official must complete the additional audit within two days after the precincts are selected and report the results immediately to the county auditor. If the second audit in any of the reviewed precincts also indicates a difference in the vote totals compiled by the voting system that is greater than one-half of one percent from the result indicated by the postelection audit or greater than two votes in a precinct where 400 or fewer voters cast ballots, the postelection audit official must conduct an audit of the ballots from all the remaining precincts in the jurisdiction for the races indicated in subdivision 3. This audit must be completed and the results must be reported to the secretary of state within one week of completing the second audit.

(b) If the results from the jurisdictionwide audits clearly indicate that an error in vote counting has occurred, the secretary of state must notify the postelection audit official that they must conduct a manual recount of all the ballots in the jurisdiction for the affected office using the procedure established in section 204C.35. The recount must be completed and the results reported to the appropriate canvassing board within two weeks of receiving notice from the secretary of state.

Subd. 6. **Report of results.** Upon completion of the postelection audit, the postelection audit official must immediately report the results to the county auditor. The postelection audit official must then immediately submit the results of the postelection audit electronically or in writing to the secretary of state not later than two days before the canvassing board meets to canvass the election.

Subd. 7. **Update of vote totals.** If the postelection audit under this section results in a change in the number of votes counted for any candidate, the revised vote totals must be incorporated in the official result from those precincts.

Subd. 8. **Effect on voting systems.** If a voting system is found to have failed to record votes accurately and in the manner provided by the Minnesota election law, the voting system may not be used at another election until it has been examined and recertified by the secretary of state. If the voting system failure is attributable to either its design or to actions of the vendor, the vendor must forfeit the vendor bond required by section 206.57 and the performance bond required by section 206.66.

Subd. 9. **Costs of audit.** The costs of the postelection audit required by this section must be allocated as follows:

(1) the governing body responsible for each precinct selected for an audit must pay the costs incurred for the audit conducted under subdivision 2 or 5, paragraph (a);

(2) the vendor of the voting system must pay any costs incurred by the secretary of state to examine and recertify the voting system; and

(3) the secretary of state must reimburse local units of government for the costs of any recount required under subdivision 5, paragraph (b).

Subd. 10. **Time for filing election contest.** The appropriate canvass is not completed and the time for notice of a contest of election does not begin to run until all audits under this section have been completed.

Ranked Voting Guidelines

Chris Jerdonek, Ph.D.*

April 16, 2007
Version 1.12

Summary

This document specifies guidelines for the conduct of ranked voting elections, where ranked voting includes both instant runoff voting (IRV) for single-winner contests and choice voting for multiple-winner contests. This document includes ballot, tabulation, reporting, manual audit, and recount guidelines. The guidelines for computer tabulation and hand tabulation are treated separately where appropriate.

Contents

 To provide feedback on this document or to request the latest version, contact the author at jerdonek@gmail.com.

1 Introduction

1.1 Overview

Instant runoff voting (IRV) and choice voting are ranked voting methods designed to maximize representation of voters. This document provides procedural guidelines for conducting elections using these ranked voting methods. In California, these guidelines are consistent with the IRV roadmap of Alameda County [AC] and the ranked voting provisions in the charters of Oakland [Oak] and San Francisco [SF]. However, any jurisdiction may adopt these procedures.

1.2 Instant runoff voting

Instant runoff voting is used for single seat contests. In the United States, jurisdictions including Oakland and San Francisco refer to IRV as "ranked choice voting." Internationally, some countries call IRV "the alternative vote," and others call it "preferential voting."

IRV is a majoritarian voting method because, in the end, over 50% of participating voters elect the winner. IRV simulates a series of runoff elections in a single election. In each round of the "instant runoff," last place candidates with no chance of winning are eliminated. Voters for those candidates have their ballot count towards their next choice in the following round.

1.3 Choice voting

Choice voting is used for multiple seat contests. Choice voting is also known as "the single transferable vote" (STV) and preference voting. Choice voting is a proportional method because all of the winners are elected with approximately equal percentages of the total vote. The percentage a candidate needs to win (called the "winning threshold") is the fewest number of votes that only the winning number of candidates can win. For example, a candidate in a 3-seat choice voting contest needs just over 25% to win. Together, the three winners of such a contest represent over 75% of the participating voters. Choice voting is designed to have as many voters as possible have their one vote count towards the election of a candidate.

2 Ranked Voting Elections

2.1 General provisions

Ranked voting elections to fill one or more seats shall conform to the guidelines in this document wherever possible.

2.2 Definitions

The following definitions shall apply to this document.

(1) "**Ballot group**" means a subset of ballots cast in an election, such as all ballots cast by voters in one precinct, or all ballots cast on one direct recording electronic (DRE) voting machine (cf. [EC]). Election officials use ballot groups for hand tabulation, auditing, reporting, and recount purposes.

(2) "**Choice voting**" means ranked voting for multiple-winner contests.

(3) "**Continuing candidate**" means a candidate who has not been eliminated.

(4) "**Continuing total**" means the sum of all continuing candidate totals.

(5) "**Instant runoff voting**" means ranked voting for single-winner contests.

(6) "**Ranked vote,**" or simply vote, means the selections made by a voter at every available ranking for a single ranked voting contest.

(7) "**Round**" means a stage of the tabulation of a ranked voting contest in which votes may be transferred and counted, and candidates elected or eliminated.

3 Ballots

3.1 Voter instructions

Ballot instructions shall direct voters to rank candidates in order of preference by choosing a first choice candidate, a different candidate for the second choice, a different candidate for the third choice, and so on. The instructions shall say that voters can rank as few or as many candidates as they want, up to the allowed limit. The instructions should convey that ranking additional choices will not hurt a voter's higher-ranked choices.

3.2 Number of rankings

The ballot format should allow voters to rank all the candidates appearing on the ballot for that contest. In addition, the ballot format should allow voters to rank a number of qualified write-in candidates equal to at least two or the number of seats, whichever is greater.

3.3 Exceptions for equipment limitations

If the voting equipment or procedures available to the jurisdiction cannot feasibly accommodate the number of rankings in Section 3.2, the number of rankings and write-in rankings may be limited to the maximum number feasible. However, the total number of rankings per ranked voting contest shall never be less than three, and voters shall always be allowed to rank at least two qualified write-in candidates per ranked voting contest.

3.4 Uniformity across ballot types

If more than one type of voting equipment or ballot will be used in a ranked voting contest, all equipment and ballot types used shall provide substantially similar instructions and shall allow voters to rank the same number of candidates and write-ins.

4 General Tabulation Provisions

4.1 Determination of winners

To determine the winners of a ranked voting contest, apply to the ballots the tabulation method of Section 5 or Section 6, depending on whether the number of seats to fill is one or more than one, respectively.

4.2 Summary reports

Election officials shall make available to the public a summary report for each ranked voting contest. The report shall display, in grid form, the following for each round: the winning threshold; the candidate totals; the continuing total; and the undervote, overvote, and exhausted vote totals. The summary report may also display, for each round, the net change of each of these values from the previous round. The summary report may also display, beside each candidate total, the candidate total as a percentage of the continuing total. Election officials shall release preliminary summary reports and are encouraged to update them regularly as more ballots are processed. Election officials should make the first preliminary summary report available on election day, if possible.

4.3 Skipped rankings

When a skipped ranking is encountered on a ballot during the tabulation of a ranked voting contest, that ballot shall count towards the next non-skipped ranking.

4.4 Undervotes, overvotes, and exhausted votes

The following rules shall be applied during the tabulation of a ranked voting contest. In the event that a ranked vote has no candidates selected at any ranking, that ballot shall

count as an "undervote." In the event that a ranked vote advances to a ranking with more than one candidate selected, that ballot shall count as an "overvote." In the event that a ranked vote is neither an undervote, overvote, nor counting towards a candidate, that ballot shall count as an "exhausted vote." Any ballot counting as an undervote, overvote, or exhausted vote shall remain so and shall not count towards any candidate in that round or in subsequent rounds.

4.5 Resolving ties

4.5.1 Standard method

In the event that a tie occurs during the tabulation of a ranked voting contest, the tie shall be resolved in public by lot.

4.5.2 Alternative method*

The following method may be used in place of the method above to resolve those ties not covered by state law that may occur during the tabulation of a ranked voting contest. Prior to election day, election officials shall draw the names of all candidates and qualified write-in candidates at random during a public ceremony. Election officials shall make the drawn order public prior to election day. In the event that a tie occurs during the tabulation, election officials shall resolve the tie in favor of the candidates appearing earliest on the publicized list. **[We do not know if the method described in this paragraph is a legal way to resolve ties under state law. This needs to be checked before including this paragraph.]*

4.6 Publicizing tabulation procedures

In advance of the election, election officials shall make available to the public a description of the tabulation procedures for each ranked voting contest. The description shall be precise enough to permit the creation of a computer program that implements the tabulation algorithm actually used. Alternatively, the public description may include a computer program with source code that carries out the tabulation algorithm actually used.

5 Instant runoff voting

5.1 Overview

Instant runoff voting is a majoritarian voting method designed to accommodate more than two candidates seeking a single seat. The ballots are counted in a series of rounds. Every voter has one vote in each round of counting, but can rank more than one candidate. The weakest candidate is eliminated after each round of counting, and each ballot cast for that candidate is counted in the next round for the candidate ranked next on that ballot. Once the field is reduced to two, the candidate with more votes is declared the winner.

5.2 Tabulation method

Election officials shall tabulate the ballots in rounds, according to the following steps.

(1) **Initial counting.**

Begin round one.

Count each ballot as a vote for the first choice candidate on that ballot.

(2) **Determine if there is a winner.**

If there are exactly two continuing candidates, declare the candidate with the larger total the winner and end the tabulation.

Otherwise, begin a new round and proceed to the next step.

(3) **Eliminate last-place candidate.**

Eliminate the continuing candidate with the smallest total. For each ballot that counted towards the eliminated candidate, count it towards the vote total of the highest-ranking continuing candidate on that ballot.

(4) **Subsequent counting.**

Go to Step (2), and continue counting ballots in this fashion, transferring votes from eliminated candidates, round after round, until only two candidates remain and the candidate with the larger vote total is declared the winner.

5.3 Elimination of more than one candidate at a time

In order to reduce the occurrence of ties that need to be broken, candidates who have no mathematical chance of winning shall be eliminated simultaneously as follows. Before Step (3), in the event that any candidate total exceeds the sum of the totals of all continuing candidates with a smaller total, eliminate all the candidates with a smaller total, count those ballots as in Step (3), and proceed to Step (4). When applying simultaneous elimination, eliminate the largest group possible that leaves at least two continuing candidates.

5.4 Voting equipment accommodation

Tabulation equipment, including software, that terminates the count as soon as one candidate has a majority of the continuing total shall be considered to be in substantial compliance with these procedures for the purposes of Section 10. However, continuing the tabulation until only two candidates remain is encouraged.

6 Choice voting

6.1 Overview

Choice voting is a proportional voting method for contests with more than one seat. The ballots are counted in a series of rounds. Every voter has one vote in each round of counting, but can rank more than one candidate. Candidates win if they reach a winning threshold. In each round, votes in excess of the winning threshold are called surplus votes and are later counted at a fractional value towards the next choices on those ballots. Moreover, in each round, the candidates that cannot win are eliminated, and each ballot cast for those candidates is counted in the next round for the candidate ranked next on that ballot.

6.2 Definitions

The following definitions shall apply to this section.

(1) "**Candidate surplus**" means the candidate total minus the winning threshold if the candidate has been declared a winner.

(2) "**Surplus total**" means the sum of all candidate surpluses.

(3) "**Winning threshold**" means the smallest whole number larger than the result obtained by dividing the sum of all candidate totals (the continuing total) by one more than the number of seats. For example, if the number of seats is two and the continuing total is 900, then the winning threshold is 301.

6.3 Precision

All vote totals shall have the same number of digits after the decimal point. This number of digits shall be determined prior to the election and made public in accordance with Section 4.6.

6.4 Tabulation method

Election officials shall tabulate the ballots in rounds, according to the following steps.

(1) **Initial counting.**

Begin round one.

Count each ballot as one vote for the first choice candidate on that ballot.

Compute the winning threshold.

(2) **Determine if there are winners.**

Declare as a winner any candidate whose total equals or exceeds the winning threshold. If the number of candidates declared winners equals the number of seats, end the tabulation.

Otherwise, begin a new round and proceed to the next step.

(3) **Transfer surplus from winning candidate.**

If some candidate has a surplus of votes above the winning threshold, then for each ballot counting towards the winning candidate with the largest surplus, count it towards the vote total of the highest-ranking continuing candidate on that ballot that has not been declared a winner. Count each ballot at a fractional amount equal to its current value times the surplus of the winning candidate divided by the total of the winning candidate.

(4) **Eliminate last-place candidate.**

If no candidate has a surplus, then eliminate the candidate with the smallest vote total. For each ballot that counted towards the eliminated candidate, count it towards the vote total of the highest-ranking continuing candidate on that ballot that has not been declared a winner. Count each ballot at its current value. If at least one candidate has already been declared as a winner, keep the winning threshold the same. Otherwise, recompute the winning threshold to account for the new continuing total.

(5) **Subsequent counting.**

Go to Step (2), and continue counting ballots in this fashion, transferring surplus votes of winning candidates followed by votes from eliminated candidates, round after round, until all seats are filled.

6.5 Elimination of more than one candidate at a time

6.5.1 To reduce the occurrence of ties

In order to reduce the occurrence of ties that need to be broken, candidates who have no mathematical chance of winning shall be eliminated simultaneously as follows. Before Step (4), in the event that no candidate has a surplus and some candidate total exceeds the sum of the totals of all continuing candidates with a smaller total, eliminate all the candidates with a smaller total, count those ballots as in Step (4), and proceed to Step (5). When applying simultaneous elimination, eliminate the largest group possible that leaves at least as many continuing candidates as there are seats.

6.5.2 For easier tabulation

In order to keep votes whole as much as possible, simultaneous eliminations may be performed as follows. Before Step (3), in the event that any candidate total exceeds the

surplus total plus the sum of the totals of all continuing candidates with a smaller total, eliminate all the candidates with a smaller total, count those ballots as in Step (4), and proceed to Step (5). When applying simultaneous elimination, eliminate the largest group possible that leaves at least as many continuing candidates as there are seats.

6.6 Order of winners

The candidates declared as winners in Step (3) of Section 6.4 shall be declared winners in order of their vote totals, with candidates having the largest totals declared winners first.

6.7 Termination of tabulation

In Step (2) of Section 6.4, if the number of continuing candidates equals the number of seats, then declare all continuing candidates as winners. If the number of continuing candidates equals one more than the number of seats, then declare all continuing candidates as winners except for the continuing candidate with the smallest vote total.

7 Computer Tabulation Provisions

7.1 General provisions

This section shall apply only to ranked voting contests tabulated by computer.

7.2 Definitions

The following definitions shall apply to this section.

(1) "**Image,**" or ranked vote image, means any alpha-numeric representation of a ranked vote.

(2) "**Raw image**" means an image captured from a ranked vote, recorded, and tallied during the tabulation.

7.3 Automatically captured ranked votes

Raw images captured from ranked votes using only automatic means, such as by optically scanning a cast paper ballot, shall indicate all candidate selections at each ranking, including skipped rankings, multiple selections of the same candidate, and multiple selections of candidates at a single ranking.

7.4 Basis for tabulation

The list of raw images shall be used as the basis for the tabulation of a ranked voting contest. The list of raw images shall be preserved on a digital medium at least until after the end of the terms of the offices being elected, and until after the end of the statute of limitation for any civil or criminal action that may arise from conduct related to casting or tabulating votes in the election, or longer, as may be provided by law.

7.5 Ranked vote image reports

7.5.1 Time and mode of release

An image report for each ranked voting contest shall be made available to the public via the Internet and by other means. Preliminary image reports shall be released and updated regularly as more ballots are processed. The first image report shall be made available on election night, if feasible. Each image report shall be accompanied by a preliminary summary report obtained by tabulating the ranked votes corresponding to the images in the image report.

7.5.2 Content

Each image report shall contain a vote image for each ballot processed up to that point. Each image in the report shall be accompanied by a label indicating whether the image was created using automatic means, such as by optically scanning a cast paper ballot, or using manual means, and by labels sufficient to designate the ballot group of that ballot, which may include labels for the precinct of origin, whether the ballot was cast absentee, and labels for any other characteristics necessary for the conduct of the public manual audit. It shall be possible to generate the summary report by tabulating the images contained therein using the tabulation method publicized in accordance with Section 4.6.

7.5.3 Ballot secrecy

The order in which images are listed in each image report shall not be related to the order in which the corresponding ballots were cast. To ensure ballot secrecy, each image in an image report can, but need not, be identical to its corresponding raw image tabulated in accordance with Section 7.4.

7.5.4 Format

Each image report shall be made available in a human-readable plain-text format. The format shall be consistent and easily described, such as comma-delimited. To permit the preparation of a computer program that can process the images in each image report, a precise description of the format of the image report shall be made available to the public in advance of the election.

7.5.5 Rules for converting ranked votes

The rules for converting ranked votes to images presentable to the public in an image report shall be made available to the public in advance of the election. The rules shall cover manually and automatically-captured images, as well as the treatment of remade ballots. The rules shall include the transcription rules for marks for write-in candidates, rankings containing more than one mark, write-in marks for ballot-qualified candidates, and other special cases. The rules shall also include any transformation rules used to protect ballot secrecy.

7.6 Public manual audit

The final image report shall be released prior to the random selection of ballots for the public manual audit. The public manual audit shall check that the images in the final image report match the ranked votes for the ballots in the randomly selected ballot groups, after applying the rules of Section 7.5.5 as necessary.

7.7 Recounts

A full or partial recount shall proceed by recreating the raw images from the original ranked votes in all of, or a designated portion of, the ballot groups. The images for these ballot groups shall be replaced in the list of raw images, and the list of raw images shall be retabulated. Image reports and summary reports shall be rereleased for these retabulations using the same procedures as for the original count.

7.8 Statement of votes cast

The statement of votes cast for a ranked voting contest shall include a summary report and the tabulation method description. An electronic statement of votes cast shall also include the final image report.

8 Hand Tabulation Provisions

8.1 General provisions

This section shall apply only to ranked voting contests tabulated by hand.

8.2 Comprehensive reports

Election officials shall make available to the public, via the Internet and by other means, a comprehensive report for each ranked voting contest. The comprehensive report shall list, for each round, the total vote from each ballot group counting towards each candidate total and counting towards the undervote total, overvote total, and exhausted vote total.

8.3 Public manual audit

For the public manual audit, election officials shall generate a comprehensive report and make it available to the public prior to the random selection of ballot groups to be checked by the public manual audit. The public manual audit shall verify for the randomly selected ballot groups the vote totals reported in the comprehensive report.

8.4 Recounts

A recount shall proceed by recounting the totals reported in the comprehensive report for all of, or a designated portion of, the ballot groups, beginning with the first round totals and continuing with later round totals as necessary.

8.5 Statement of votes cast

A statement of votes cast for a ranked voting contest shall include a summary report, a comprehensive report, and the tabulation method description.

9 Voter Education

Any jurisdiction using ranked voting shall conduct a voter education campaign to familiarize voters with ranked voting. Voter education shall include outreach to speakers of all languages used on ballots in the jurisidiction.

10 Changes to Procedures

Election officials may change the procedures described in this document to accommodate the voting equipment available, provided that the new procedures are in substantial compliance with the procedures described here, the smallest feasible number of changes is made, and the changes to the tabulation procedures are made public in accordance with Section 4.6.

11 Voting Integrity and Ballot Secrecy

The procedures described in this document provide a robust audit framework that supports software independence and maximum transparency, while still protecting ballot secrecy. One component of this audit framework is to make both the tabulation algorithm and input to that algorithm public, for computer-tabulated elections. This allows anyone to verify that the computer is carrying out the tabulation algorithm correctly. The input data made public is called an image report. The second component of this framework is to randomly audit the final image report in a public manual process. The manual audit directly checks that

the publicly released data matches the original paper ballots and/or voter-verified paper audit trails (VVPATs). Taken together, these steps ensure election integrity. The third component protects ballot secrecy. The notions of raw and publicly reported images in Section 7 ensure that votes can always remain anonymous.

References

[EC] California Elections Code, Section 15360, as of March 2007.

[Oak] "The Charter of the City of Oakland," Article XI: Elections, following passage of Measure O charter amendment in November 2006 entitled "Ranked Choice / Instant Runoff Voting."

[SF] "City and County of San Francisco 1996 Charter," Article XIII: Elections, Sec. 13.102. Instant Runoff Elections, as of March 2007.

[AC] "Final Draft IRV Roadmap," Alameda County Acting Registrar of Voters Elaine Ginnold and Alameda County Instant Runoff Voting Task Force, August 12, 2005.

Appendix V: FairVote Comments on TGDC's VVSG

Specific Recommendations to the VVSG

4.4.1-A.9 IVVR vote-capture device, IVVR unambiguous interpretation of cast vote

Each IVVR SHALL contain a human-readable summary of the electronic CVR. In addition, all IVVR SHALL contain audit-related information including:

a. Polling place;
b. Reporting context;
c. ballot configuration;
d. Date of election; and
e. Complete summary of voter's choices.

In regards to 4.4.1-A.9, FairVote believes the requirement that an optical scan or other electronic vote capture device store a Cast Vote Record (CVR)- that is a ballot image rather than tabulating voter selections- is a positive development in the VVSG. However, we disagree with the use of the word "summary" in describing the complete record of voter choices. Instead, we suggest replacing the word "summary" with "record."

Secondly, while the requirements for IVVR systems, such as VVPAT, clearly require that the CVR contain a complete record of each choice made by the voter, it is not clear in the current TGDC's recommended VVSG that ALL systems are required to store this information. We believe all vote capture devices should store and output Cast Vote Records that include a separate record for each contest and each "ballot" with a complete record of each choice made by the voter.

7.7.2-A.17 Tabulator, ranked order voting

Tabulators of the ranked order voting device class SHALL be capable of determining the results of a ranked order contest for each round of voting.

Instead of the current guideline, this should read:

"Tabulators of the ranked order voting device class SHALL be capable of determining the results of a ranked order contest for each round of vote tabulation."

We believe this is the correct wording since there is only a single round of voting in a ranked order voting election, but potentially more than one round of vote tabulation.

7.7.2.5 Logic for ranked order voting

Although we agree that it might be premature to standardize algorithms and other logic for ranked choice voting systems, it is overdue for the EAC to convene an advisory or working group to explore options and begin the process of developing standards. Major voting machine vendors such as ES&S and Sequoia already have, or are currently in the process of having voting systems for ranked voting tested and certified by laboratories. The absence of federal guidelines in this area is a major problem for both vendors and jurisdictions that have adopted ranked voting methods. It would be appropriate to have a two-step set of guidelines; containing both minimum standards for retrofitting legacy equipment, and best-practice standards for future products. Premier Election

Systems (Diebold), ES&S, and Sequoia have all produced firmware to handle ranked voting on some of their existing machines. However, none of these machines are using what the advocacy community considers to be best practices. For example, ideally the output from the vote capture device should be a true representation of all voter choices made, regardless of validity (e.g. rather than inserting a generic "over-vote" code the output should show exactly what choices the voter made), and leave it to the subsequent step of vote tallying software to interpret those voter "marks." All three of these vendors have produced firmware for their optical scan machines that somewhat "cleans" the data that it outputs (such as skipped rankings or duplicate rankings, etc.). This makes auditing a ranked ballot election problematic, as there is no longer a one-to-one match up of ballot to data record. Thus a best practice for future systems would require that the vote capture device store anonymous un-interpreted ballot images from each voter. Also the output file should be in a common record format, such as a comma delimited text file rather than a proprietary format, to allow double checking algorithms by running the ranked ballot election through software other than just that provided by the vendor.

7.8.3.3-D Ranked order voting, report results

Systems conforming to the ranked order voting class SHALL report the contest choice vote totals for each ranked order contest for each round of voting/counting at the system extent level.

Currently, these guidelines may be sufficient for ranked choice voting jurisdictions to report results. However, we believe these guidelines should eventually require polling sites or at least on the precinct level to report the number of first preferences for each contest choice. In the long term, the precinct machine should be able to print a total of each of the rankings received by each of the contest choices. This information is not useful for tallying the election, to know who won, but is a security function to allow a complete audit after the election is completed. None of the major vendors currently have this capacity, but future systems should be required to have this capability.

Glossary Definitions

Voting system: Equipment (including hardware, firmware, and software), materials, and documentation used to define elections and ballot styles, configure voting equipment, identify and validate voting equipment configurations, perform logic and accuracy tests, activate ballots, capture votes, count votes, reconcile ballots needing special treatment, generate reports, transmit election data, archive election data, and audit elections. See also, voting process.

We believe this definition needs further clarification. Does a voting system as defined need to contain all of the above elements or could a voting system still be defined as such without the capabilities (i.e.) of transmitting election data. Additionally, in section 6.1-C

6.1-C Voting system, minimum devices included
Voting systems SHALL contain at least one EMS and at least one vote-capture device.

a “voting system” if further defined as requiring both and EMS and a vote capture device. The EAC should provide a clear and concise definition of what a voting system entails.

Written Testimony of John Washburn

Representing VotersUnite!

General Observations

The primary premise behind the creation of the 2007 VVSG is the belief that these standards will be enforced when they become active in 2012. Five years of recent evidence indicate this will not be the case. Current, known violations of the 1990 and 2002 voting systems standards have resulted in no sanctions or recalls for the deployed systems that were approved under those standards and yet exhibit such defects.

The second premise is that the design requirements laid out in the various Voluntary Voting System Guidelines can be considered in isolation from the rest of the EAC structures being created, such as the Quality Monitoring Program, the Testing and Certification Program, and the National Voluntary Lab Accreditation Program for Voting System Test Labs. These structures as currently designed do not work together and, in fact, seem to have been designed, each in isolation from the others. I would urge the Election Assistance Commission, the National Institute of Standards and Technology, and the Technical Guidelines Development Committee to consider as a whole the various pieces and parts of the proposed regulatory framework of elections.

Enforcement Concerns

The EAC has neglected its HAVA mandated role to be a clearinghouse of information on voting systems. This duty is laid on the EAC under Section 202 paragraph (3) of the Help America Vote Act which reads:

> *The Commission shall serve as a national clearinghouse and resource for the compilation of information and review of procedures with respect to the administration of Federal elections by —*
>
> *(3) carrying out the duties described in subtitle C (relating to conducting studies and carrying out other activities to promote the effective administration of Federal elections);*

Subtitle C is entitled [emphasis mine] *Studies and Other Activities To* ***Promote Effective Administration of Federal Elections,*** and the pertinent portion of subtitle C to the EAC role as a clearinghouse is Section 241 paragraph (a)(2) which reads:

> *On such periodic basis as the Commission may determine, the Commission shall conduct and make available to the public studies regarding the election administration issues described in subsection (b), with the goal of promoting methods of voting and administering elections which –*
>
> *(2) will yield the most accurate, secure, and expeditious system for voting and tabulating election results;*

Presently, the only clearinghouse of information on actual system faults found in currently fielded voting systems is maintained on a volunteer basis by VotersUnite and can be found on the website http://www.VotersUnite.org. In the last year, the EAC has been notified of at least two serious defects found in voting systems used across the county, and in both cases the EAC declined to warn affected election officials of the existence of these defects. The first defect is the smoothing filter problem found on the iVotronic touch screen DRE. While this problem was discovered in Florida, the particular version of iVotronic software is used around the country and in Taylor County of my home state of Wisconsin. The town and municipal clerks are unaware of the smoothing filter defect found in the software they use to administer elections. The second problem that the EAC has declined to publicize is the scanning defect in the AccuVote OS manufactured by

Premier Election Systems. With this defect, the paper ballot is fed into the front of the scanner and deposited in the lock box below without registering that a ballot has been cast. This defect was reported by Premier itself as a product advisory, but only to selected counties in Florida. This particular system fault is of particular interest to me because I observed the fault in both the November 2, 2004 and April 5, 2005 elections in my home voting location: District 1 of the village of Germantown, Wisconsin. My village and county clerk deserve to be told that there is a known defect in the voting system they have chosen to administer elections. Prior to these two faults was the discovery of interpreted code in both the Diebold scanner and DRE systems. Interpreted code is explicitly prohibited by the 2002 VVSG. Each of these defects can and have led to inaccurate election results.

Recently, VotersUnite has begun tracking a new category of system fault. Section 301(a) of HAVA has few requirements for a voting system used in a federal election, but one of them is the accuracy requirement found in §301(a)(5). This paragraph of HAVA requires a voting system have a maximum error rate of no more than one error per 500,000 ballot lines scanned. VotersUnite's tracking so far shows that this accuracy requirement has been violated by systems from at least four different manufacturers.

The official position of the EAC is that since these faults are in systems which are not certified by the EAC, the Commission has no duty to report on such systems. Since the EAC has taken no action on reported violations of §301(a)(5), it appears that the Commission also believes it has no duty to decertify systems that violate HAVA mandates.

The EAC will not carry out the simplest of its HAVA-mandated duties: reporting on currently fielded voting systems. It is truly faith (the belief in things not seen) which would lead one to believe the EAC will do the much more difficult task of enforcing standards.

Isolation of Technical Programs

Elections take place in a complex technical, social, political, and legal environment. The consideration of the VVSG is on the purely technical aspects of voting machinery. This is a mistake. This fragmenting of duties and isolation regarding the technical aspects will be taken up in more detail below.

On the wider, non-technical aspects of elections and the voting machinery used to administer them, consider Sarasota County , Florida. During .the November 6, 2006 election in Sarasota County, Florida, 18,000 votes for Congressional District 13 are unaccounted for. The speculation of the Supervisor of Elections of Sarasota County is that 18,000 voters deliberately skipped this high profile race. The speculation of one candidate, Christine Jennings, is that the voting machinery faulted in some manner which resulted in the loss of the votes cast by 18,000 voters. Unfortunately, the voting machinery in question is so poorly designed that it provides evidence that supports the speculation of either the Supervisor of Elections or the contesting candidate. Moreover, there is no way to resolve this uncertainty, so the question can only linger and fester.

Had the technical community recognized the larger social, political, and legal context of elections, this uncertainty could have been eliminated. If an election is to capture the complete spectrum of possible consent options from the governed, then the ballot should contain options for:

- Pre-printed candidates (or their electors)
- Write-in candidates whether certified or not
- None of the Above; New Election (i.e. neither candidate is acceptable)
- None of the Above; Abstain (i.e. either candidate is acceptable)

Under the Times and Manners clause of the Constitution, Congress could require for all federal contests that all consent options be present and that a voter in a federal contest must select one and only one of the consent options available. Every voting system currently fielded today can implement this requirement. Had such a requirement been in place on November 6, 2006, then there would not have been any uncertainty in Sarasota County Florida. Either there would be 18,000 missing votes (a clear system fault) or there would be 18,000 votes distributed among the write-in option and the two NOTA options.

This is not the official position of VotersUnite, nor is it a recommendation from VoterUnite. The "none of the above" options described above are meant simply to illustrate that by recognizing the limits of the technology, it is possible to use the social, political, and legal aspects of the election environment to create a working election system.

But, this solution begs the question: What is a working election system? This is not a question American society has asked in over 100 years. The problem with the current VVSG structure is that it is assumes there is a consensus on what constitutes a working election system. Moreover the TDGC assumes the definition of a working election system largely ends with the hardware and software of the election machinery used to administer an election. Because of this there is little to no integration of the 2005 or 2007 VVSG with the Testing and Certification program developed by the EAC. Because of this there is little to no integration of the 2005 or 2007 VVSG with the National Voluntary Laboratory Accreditation Program for Voting System Test Labs developed by NIST.

For example, the handbook NIST-150b states that the lab accreditation program can be made more stringent based on the defects reported to the Quality Monitoring Program or a change to the underlying standards. The Quality Monitoring Program, though, has such a narrow definition of "anomaly" that it is unlikely any entry will ever be reported to the program. The open ended testing proposed by the VVSG assumes that the Voting System Test Labs will provide the information to the EAC in its role as a clearinghouse and that the EAC will provide information to the VSTL from its Quality Monitoring Program. Since the database for the EAC Quality Monitoring Program is likely to remain empty, there will be no information upon which the VSTL will have the authority to conduct the open ended testing allowed by the VVSG.

Because the pieces and parts of the proposed regulatory framework (VVSG, NVLAP, VSTL, and the EAC QMP) do not mesh, none of the pieces and parts will work as expected, if at all.

Responses to Roundtable Questions

I am pessimistic that the currently proposed election regulation framework will improve election management. The current standards in force, 2002 VVSG, have already been violated by currently fielded voting technology qualified under those standards. The 2007 VVSG (more properly the 2008 VVSG) cannot affect the voting technology of an election until at least 2012. More likely, there will be no effect until 2014. Such a long lead time between the specification of requirements and deployment to the field nearly guarantees failure.

Risk Assessment

The essential elements to consider in assessing risk for malicious action are a threat model and an attack surface. A threat model is an assessment of what kinds of threats are posed by which classes of attackers. The attack surface is an assessment of the kinds of interfaces to the system and how interactions with those interfaces affect system behavior.

The essential elements to consider in assessing risk for non-malicious action are a failure mode analysis and a reliability analysis. A failure mode analysis is an assessment of all the ways the system can fail, and a reliability analysis is an assessment of the likelihood of each failure mode.

These are two kinds of risk: malice and mistake. For each risk, there is already a well established framework for making the risk assessments. That the best practices of neither the security community (risks posed by malice) nor reliability engineering (risks posed by mistake) has been applied to election technology is a testament to how ill-conceived the technological mandates of HAVA have been implemented.

Open-Ended Vulnerability Testing

Open ended vulnerability testing is very valuable in a software system that is also expected to be either a high reliability system or a highly secure system. Election software systems are expected by many to be both highly reliable and highly secure. Any of the risks associated with performance of the open ending testing are more than outweighed by the benefits such testing brings by uncovering defects which compromise security or reliability. The smallest benefit such testing brings is simple information on how a system is unreliable or how a system is vulnerable to manipulation. In the case of administration, knowledge is power. If you are unaware of a failure mode or manipulation potential, you will neither watch for it nor guard against it.

While the inclusion of the open ended vulnerability testing in the 2007 VVSG is a welcome addition, there is no need to wait until 2010 or beyond to perform such testing. The EAC has had the authority since 2002 to conduct and supervise such testing. Section 241(b)(19) of the Help America Vote Act has already given the EAC the authority to conduct or to sponsor such testing at any time since the legislation was enacted.

The best way the EAC could enact open-ended vulnerability testing is to immediately sponsor the work of the University of Connecticut, Princeton, MIT, UC Berkeley, and others that are already doing the open ended vulnerability testing the EAC claims it wants to conduct.

Test Methodologies

Test methodologies already exist which would ensure voting systems are high-reliability systems. High-reliability techniques are used in both avionics and health care. Until such methods are applied to voting

technology, voting technology will continue to be poorly designed and unreliable. Until it is recognized that failed election administration carries risks at least as high as failed medical or avionics technology, there will be no incentive to apply the proven techniques of high-reliability design to election technology.

Conflicting Needs

The perception that there are conflicting design goals for voting technology stems from the fact that Americans as a body politic have no consensus on the virtues to be preserved in an election or a consensus on the priority of those virtues. Here are examples of virtues for an election, presented in no particular order.

- Observable by Citizens
- Re-countable
- Auditable
- Accurate – Correctly identifies and reports votes
- Correct – Correctly administers applicable election law
- Usable – Election Official
- Usable – General Voter
- Usable – Voter Language
- Usable – Physical Disability
- Usable – Cognitive Disability
- Secure from Manipulation – Election Officials
- Secure from Manipulation – Political Parties
- Secure from Manipulation – Voters
- Secure from Manipulation – Other

The needs are conflicting to the technology design because there is no consensus in the larger social, political, and legal worlds as to what is a successful election. It is not the place of the TDGC to balance these needs and election virtues. An evaluation of the technical options available cannot be made until a rough consensus in the political, legal, and social world has emerged.

Conclusions

The 2007 VVSG is part of a continuing pattern of distracting attention from current problems in election administration by proposing a technological fix to a failed technology and then postponing the deployment of that new technology to the distant future. Five years in elections is the distant future. The current 2005 VVSG is already obsolete. This new standard applies to no system currently on the market. But, because the 2005 VVSG does not .incorporate the latest information discovered over the last year by open ended testing done by volunteers and states, voting systems can carry these known defects forward and still meet the requirements of the 2005 VVSG.

To a large degree technology is not the solution to the problem. Technology is the problem.

The Election Assistance Commission has the authority ***NOW*** to alleviate most of the election administration ills addressed by the 2007 VVSG.

The EAC can and should document known defects found in currently fielded systems. The EAC should publish those defect reports on a public web-site. The EAC should also pro-actively contact the affected jurisdictions when a new defect is discovered. In short, the EAC should be a clearing house for information on election technology used to administer elections. This is one of the primary duties the Congress mandated to the EAC via the Help America Vote Act. It is a duty the EAC has yet to fulfill.

The EAC can and should exercise its authority under §241 of the Help America Vote Act to sponsor and expand the open ended vulnerability testing already being done on a volunteer basis by citizens and universities.

In short, even if the 2007 VVSG specified high-reliability technology, the fact is that the EAC is unlikely to enforce the standards. Because of this, some time in 2015 we will realize the 2007 VVSG was a wasted effort and that we have lost 5-7 years engaged in yet another dysfunctional voting system certification process. We can better spend this time addressing, and possibly improving, election administration in the context of political, legal, and social realities.

America's Elections Watchdog Group

Black Box Voting • org

EAC VOTING ADVOCATES ROUND TABLE: April 24, 2008

Request that the following comments be entered into the record on behalf of Black Box Voting, by its founder, Bev Harris.

To members of the EAC and participants of the Round Table:

The entire premise of technology-based elections is based on support for the "verifiable voting" concept. But before designing technology for elections, we must first determine how it will empower citizen controls, enabling the counting of votes in public rather than counting them in secret. We do not consent to any form of secret vote counting that is administered and controlled by government insiders and their vendors.

Any system that forces the citizenry to trust government insiders to count their votes represents a change in the original design of this nation. The United States of America was designed to uphold the right of citizen sovereignty over the government. In addition to hiding the counting of votes from public view, computer-counted elections hide the chain of custody of the vote data. Citizens are never allowed to view the original input in order to compare it to the output, and are relegated to trusting circumstantial evidence controlled by insiders. Such a system is, in fact, a transfer of power.

The people were never asked to approve such a transfer of power, have never consented to it, and indeed *cannot* consent, because the right of sovereignty over the instruments of government which we have created is an inalienable right, one which *cannot* be given away, nor can this right be removed through legislation. It is, admittedly, possible for a government to decline to honor this right, but such an act would justify extreme measures by the people subjected to such abuse of power.

It is the public counting that is key to citizen sovereignty, not computer verification. "Verification" of a computer report is not at all the same as public vote counting.

The core of elections was and again must return to the principle of citizen sovereignty over government. Elections can never be based on a requirement to trust government insiders and their vendors to count our votes, nor can elections be dependent on experts to tell the citizenry that the system is okay, nor should the detailed mechanics of elections be impossible for the average citizen to understand. Models which depend on experts and insiders create centralized control, and remove all control from government's rightful owners – the citizens. This represents a violation of the principles laid out in the Declaration of Independence.

Not only does my organization, Black Box Voting, refuse to participate in the design of such systems, but we will do our utmost to inform the populace that such systems must be revoked, by whatever means necessary.

"We do not consent."

Bev Harris
Black Box Voting
330 SW 43rd St Suite K
PMB 547
Renton WA 98057

STATEMENT OF BRAD FRIEDMAN
Publisher/Editor, The BRAD BLOG (www.BradBlog.com)
Co-Founder, VelvetRevolution.us

FOR

THE U.S. ELECTION ASSISTANCE COMMISSION'S
"VOTING ADVOCATE" ROUNDTABLE DISCUSSION
ON PROPOSED 2007 VOLUNTARY VOTING SYSTEM GUIDELINES
THURSDAY, APRIL 24, 2008

* * *

I wish to thank the EAC for extending an invitation to The BRAD BLOG to participate in today's roundtable discussion. The effort to reach out to citizen election integrity advocates is long overdue for this commission. I hope that this meeting will be just the first step, as long as this body remains commissioned, towards an increased effort to begin welcoming the most important stakeholders in our elections – the citizens themselves – into a process that has, since the EAC was convened via the Help America Vote Act of 2002, remained far too long as the near-exclusive domain of those who profit from it, and those who have been tasked with administrating our elections as servants on behalf of those citizens.

While being asked to offer input, from a "Voting Advocate" standpoint, on the proposed 2002 federal Voluntary Voting System Guidelines (VVSG), I was immediately struck by the 598 pages of technical specifications for new electronic voting systems. While nearly complex enough to ensure safe passage to the moon and back, the proposed standards, unfortunately, fail to offer the simplicity and transparency necessary for the simple task of adding one plus one plus one, in such a way that *every* American citizen can enjoy confidence that their voting system works, and that every vote has been counted -- *and counted accurately* – to each voter's intent.

I should note that counting votes accurately, in and of itself, is not enough if only a select group of privileged corporate insiders, elected or selected government officials, or computer scientists, engineers and security "experts", are granted permission to review data unavailable to the general public.

Accurate vote counts are ultimately meaningless if we, the people, are unable to know that they are, indeed, accurate.

Confidence in the accuracy and security of voting systems, as attested to by only selected, privileged individuals, cannot -- and must not -- ever be tolerated as a substitute for the rights of we, the people, to ensure our government is truly one selected of the people, by the people, and for the people.

To that end, while I applaud the assiduous and exacting attempts of the scientists, engineers and security experts of the Technical Guidelines Development Committee (TGDC) who have worked on with the National Institute of Standards and Technology (NIST) to develop the proposed 2007 VVSG, I feel it necessary to trumpet the clear and unambiguous message of all of the American citizens who are *not* computer scientists, not computer technicians, not computer security experts, not election administrators and not "election industry" corporate insiders.

While the currently proposed VVSG makes a valiant effort at dealing with crucial, yet unaddressed or poorly-addressed issues in previous sets of voluntary federal voting system standards, ultimately, the latest update serves to do little more than encourage and enable the continued use of voting devices and machinery which overcomplicate our voting process. The blizzard of technical specifications serves only to obscure the fact that, even if such specifications are followed to the satisfaction of federal testers, it will likely continue to remain next to impossible for *citizen voters* to determine for *themselves* whether or not reported election results are truly accurate.

Just as previous voluntary federal standards have enabled Election Officials around the country to point to their selected voting systems and proudly (if often cynically) declare them to be "secure and accurate", simply because they reportedly met such standards during secret testing, I am concerned that these "new and improved" standards will similarly be used to offer a *chimera* of "security and accuracy" to voting systems which, nonetheless, require blind faith in the system itself. Therefore, the message I hope deliver to you today, on behalf of election integrity advocates – otherwise known as citizen voters -- on the ground, from across the entire country is that *if we cannot see it, we cannot trust it*.

As I am unable to attend the roundtable in person, I've asked Dr. Rebecca Mercuri to represent the interests of The BRAD BLOG today, and am confident she will be able to expound on the details – specific, technical and otherwise – of how that idea translates into practical standards for any voting system worthy of our representative democracy.

In this statement, I hope to deliver the crystal-clear, unambiguous, no-uncertain-terms demand that America deserves nothing less than a transparent, secure voting system, which *every* citizen can oversee, *every* step of the way – whether or not they happen to be a computer expert, election officials, or voting machine vendor or employee -- so that we, the people, may have a fighting chance for an election system, and election results, in which we, the people, can truly grant our confidence.

I recognize that the administration of such systems, particularly at the federal level, with so many jurisdictions and legal requirements in fifty different states and thousands of counties across the country, is no simple task. I also recognize the responsibilities of the citizenry in participating in, and overseeing, the often-complicated processes and exacting standards which are necessary to ensure the private, secure, and accurately counted ballot of every citizen who wishes to exercise their franchise in an American election.

Similarly, I appreciate that various, yet limited, concessions and compromises in full voting system transparency may have to be sacrificed in order to offer accommodations for blind and disabled voters who may choose to vote "privately and independently," as HAVA requires, without the aid of a human assistant.

But while the process to accomplish all of the above may be often-complicated, it needn't be overly-complicated.

Neither must it be allowed to forever become the private property of private corporations who have alarmingly subverted the *public* process of American democracy by converting it into their own exclusive, privileged, proprietary domain.

Neither must our public servants, granted the privilege of administrating our public elections on behalf of the people, continue to enable and serve those private, proprietary interests over the public interests and rights of we, the people.

In that light, I call for an immediate end to the dangerous path this commission continues to enable in their support of the fully faith-based, privatized, proprietary, non-transparent voting systems which have disabled and deprived us -- we, the people – from being able to assure that elections results indeed represent the consent of the governed.

The Election Assistance Commission has overseen and enabled a federal process which, up until now, has granted a federal blessing to voting systems such as Direct Recording Electronic (DRE/touch-screen) devices for which it is literally impossible for *anyone* to prove that *any* single vote, ever cast on such a system during *any* actual election, for *any* candidate or initiative on the ballot, has *ever* actually been cast and recorded accurately to the intent of *any* voter.

I extend the invitation -- to *any* vendor or official, including any member or employee of this commission -- to prove otherwise, and to demonstrate that any such vote was *ever* recorded accurately during *any* American election. Even as I well understand that that proof, the minimum any citizen could ever ask for in regard to their voting system, will never come.

That such unverifiable systems are in use today -- and will be used again by *millions of voters* this November -- is an unmitigated disgrace, and underscores a massive collective failure of common-sense oversight and a nearly-unforgivable delinquency by those charged with that task at the federal level.

Such a failure is also the result of previous collective efforts by federal commissions and enabled bodies which have preceded this one, and of anyone who would allow or encourage the use of such systems in our democracy, be it this week, this November, or in any American election to come.

The very basis for our Constitutional system is one of checks and balances. Yet without the ability to apply such checks and balances, such as with the DRE systems used to record millions of votes in this year's election cycle alone, the citizens have been completely blinded and robbed of their right and ability to assure the consent of the governed.

We have been forced, for too many years now, to merely accept the pronouncements of election officials – who themselves have been forced to accept the pronouncements of flawed, error-prone, under-tested, easily-manipulated computer systems and processes which purport to count ballots, often invisibly, and almost always secretively – without having the ability to perform our constitutional right and duty of oversight for every step of the process. Without such a paramount ability, it has become nearly impossible to carry out anything that has a chance at being seen as a truly successful election.

Following the 2004 Presidential Election debacle, Green Party Presidential candidate David Cobb declared, at a citizen's hearing in Ohio: "Either every vote is sacred, or our democracy is a sham."

Unfortunately, with electronic voting and tabulation systems such as those in use across our country today -- and assured for continued use tomorrow, and for decades to come, should the mind-numbingly technical,

absurdly over-complicated, and dangerously flawed VVSG be approved and used as a basis for federal voting system certification – American democracy is certain to continue its ill-conceived sprint straight over a treacherous and damnable cliff.

We, the people, cannot possibly succeed in our efforts, and duty, to assure the sacredness of every vote, if the *secret-ness* of the very processes of counting those votes, and counting them accurately, has taken precedence over the right of we, the people (not we, the computer scientists, or we, the corporate insiders) to assure the integrity of that process and the accuracy of each and every ballot tabulated.

Without that ability, democracy surely, as Mr. Cobb stated, becomes little more than "a sham."

To that end, it's my hope that the process embarked on today will begin to lead us to back *away* from the precipice we have been sprinting toward, with alarming speed, for far too long. I hope the simple benchmark of "if we can't see it, we can't trust it," will become a siren song for all of those entrusted with the privilege of developing, creating, implementing, adopting, testing, approving and overseeing "voting technology" and systems worthy of our representative democracy.

While both Dr. Mercuri and I recognize the necessity of ensuring we, the people, *can* observe every step of the voting process (with the exception of the citizen's privileged moment while filling in, and casting their ballot), we also realize that such transparency, alone, does not necessarily translate into an automatic grant of "trust" in the system. But in the use of systems which afford such transparency, at least, we, the people, will then have a fighting chance of gaining trust in their use.

Coupled with transparent, well-documented, publicly available and fully-observable security processes and chains-of-custody for every element of the voting system, we, the people may once again be able to work to ensure that every vote *is* sacred and American democracy will no longer be seen around the world – as it too-frequently now is -- as little more than a sham.

It is with those principles in mind that we offer input towards the specific questions that you've given to us, in regard to the proposed 2007 VVSG. And it is in that spirit that we hope you, the commission, and the other esteemed "Voting Advocates" might join us in careful consideration of the questions posed, concerning the new, proposed technical specifications for voting systems, as presented by the document in question.

As mentioned, we find the document ultimately lacking in many respects, upon which Dr. Mercuri will elaborate in additional technical detail, both in her written testimony and via her personal participation at the roundtable itself.

But I'd like to offer just two concrete examples of flaws immediately noticeable, from a citizen voter's point of view, in the proposed guidelines.

The first example is found in the "Purpose" of the standards, as defined in section 3.1.1 describing the "challenge" hoping to be met by the 2007 VVSG. That challenge is said described as one "to provide a voting system that voters can use comfortably, efficiently, and with justified confidence that they have cast their votes correctly."

While such objectives are certainly worthy, the statement itself, as with much of the rest of the document, fails to even consider the simple question of whether voters can have "justified confidence" that their votes have been *counted* accurately by federally approved systems.

Comfort, efficiency and confidence in having *cast* a vote -- without the appropriate attention to whether or not "justified confidence" can be obtained by every voter that such comfortable, efficiently cast ballots have accurately been tabulated – leaves our electoral system in the same alarming shambles that it has become. How such an egregious oversight could find its way into such a document is simply beyond me.

Another example of where the VVSG falls far short of what citizens require from any federal voting system standards, is the lack of definition for the concept of "transparency" itself.

Though the word is used a precious few times throughout the 598 pages of proposed technical standards, and even though the first-named subcommittee established by the TGDC in 2004 was the "Security and Transparency" subcommittee, the concept or definition of a voting system, fully *transparent* to the *voter* for whom its designed, is nowhere to be found in the voluminous document.

While Dr. Mercuri will offer more such insight and concerns to you today, I must stress, however, that our involvement and participation in this process, may not be offered or used by the EAC or any of its sub-committees or representatives thereof – in any way, shape or form – as representing approval of this process, or endorsement of its ultimate outcome, including any version of the VVSG which may become approved for federal use by this commission.

Both Dr. Mercuri and I have extensive, and noteworthy, technical backgrounds, with considerable joint expertise in computer programming, design, security and other related issues. But today, we come to this panel in hopes of representing the voice of the *citizenry* for whom this body has been commissioned to serve.

Therefore, the concerns expressed in this statement, in initial response to your submitted technical questions, are approached of…

…the more than 12,000 citizen voters whose legally and accurately cast votes were discarded because it was inconvenient to count them after the *federally qualified* optical-scan systems, marketed by the ES&S corporation, were programmed in such a way that they could not tabulate ballots correctly during the 2008 Democratic Primary in Los Angeles County;

…the 18,000 citizen voters who were most-assuredly disenfranchised when the *federally qualified* ES&S iVotronic touch-screen systems in Sarasota County's 13th Congressional District election failed to record their votes properly in 2006;

…the thousands of disenfranchised citizen voters who saw their votes flip before their very eyes on *federally qualified* touch-screen voting systems made by Diebold and Sequoia and ES&S and other vendors all across the country in 2004, only to be told when they attempted to alert officials and media, that they were crazy, sore losers, conspiracy theorists or that it didn't really matter anyway;

…the 4,500 citizen voters who had no idea that their votes would be completely lost by the *federally qualified* UniLect Patriot voting system in Carteret County, NC that same year.

…And as importantly, if not more so, those citizens who have sacrificed their lives, over decades of American history, on these shores, and overseas, to assure that every American citizen could exercise their right to cast their legal vote, privately and independently, that every vote would be sacred, counted and counted accurately, and that American democracy might be seen the world over as anything but a sham.

In closing, I'd like to draw your attention to the mission statement constructed by a small, but diverse group of citizen election integrity advocates, including members of the media, an election official and even a vendor, who gathered recently in Northern California. Our hope in crafting the statement (I was honored to be one of the attendees) was to find common ground, and prepare for the continued, long, and eternally vigilant fight we all face to ensure the United States meets its promise as "the world's greatest democracy."

In eight simple words, certainly far fewer than 598 pages, or even the 6 pages of this document, we defined the heart of the mission I challenge all Americans – whether public servant, advocate, vendor or elected official – to join. The mission, officially adopted as "The Creekside Declaration" on March 22, 2008, as reported by both Robert Koehler in his syndicated Tribune Media Services column, and by myself at The BRAD BLOG, is simply: "To encourage citizen ownership of transparent, participatory democracy."

That ideal must underscore every effort we take today, tomorrow, and in the months and years ahead, as we all work to ensure the continued citizen ownership of a transparent, participatory democracy.

That must become *your* mission at the EAC. Meeting that ideal must underscore your adoption of any new federal voting system guidelines. *"If we can't see it, we can't trust it."* If it does not aid in the mission to "*encourage citizen ownership of transparent, participatory democracy*," it must not be adopted or implemented.

America deserves standards no lower, and we hope you will pledge to join me and millions of citizens towards those ends.

I thank you again for allowing The BRAD BLOG into this process, along with the millions of concerned citizens who follow, support and share in our work on a regular basis, and to whom we feel duty bound to give voice to today. I hope that more opportunities will arise to bring more of the stakeholders together (and we consider the *voters*, on whose behalf I hope to write today, to be the primary, yet most-ignored, stakeholders of all in this process) in hopes of finding a more productive, more constructive and less divisive path on which we can all proceed towards what I hope is the shared goal of a clean, fair, open, accurate, secure and *transparent, participatory* democracy in which we can all, one day – hopefully very soon -- have full confidence.

Brad Friedman
Los Angeles, CA
April 21, 2008

U.S. Election Assistance Commission Voting Advocates Roundtable Discussion
Thursday, April 24th, 2008

Comments of Barbara Simons
Board member, Verified Voting Foundation

I want to thank the EAC for holding this round table and for inviting me to present the views of the Verified Voting Foundation.

It is critically important to the well being of our democracy that our elections have transparency and accountability, so that Americans trust the outcomes of those elections. The draft VVSG reflects an impressive effort to establish a framework for the design, manufacture, and, ultimately, deployment of voting systems that will have transparency, auditability, and accountability. Essential to these goals are the mandates for Software Independence (SI), Independent Voter-Verifiable Records (IVVR), integratability requirements, auditing support, and usability benchmarks.

While we fully support the goal of software independence through the use of IVVR, Verified Voting recognizes a qualitative distinction between an IVVR that a voter has marked – either physically or through the use of an assistive device – and an IVVR that a voter has been given the opportunity to review. Software independence is best achieved through the use of voter marked paper ballots.

We also applaud the inclusion of Open Ended Vulnerability Testing (OEVT), which has proven valuable in identifying security vulnerabilities in numerous reviews. While testing alone cannot ensure the accuracy and integrity of elections, testing plays a vital role in efforts to improve the administration of elections. We recognize, however, that there is a point of diminishing returns. At some point, the benefits of additional testing requirements should be weighed against the costs, which could include reduced choices of voting equipment available to election officials and voters, as well as longer delays in introducing improved equipment.

The limitations and costs of testing make the mandates for Software Independence and IVVRs even more imperative. Effective independent auditability is precisely what mitigates the inherent inadequacy of the testing and certification process, and we strongly urge the EAC to retain these TGDC recommendations.

Responses to Questions

1. *On October 7, 2005 the National Institute of Standards and Technology (NIST) held a "Risk Assessment Workshop" in order to evaluate threats to voting systems. The results of that workshop can be found at http://vote.nist.gov/threats/. In so doing NIST recognized the importance of evaluating threats when developing a secure voting system, but no formal risk assessment was developed. The EAC is now interested in learning how to best develop a risk*

assessment framework to provide context for evaluating the security implications of using various technologies in voting systems?

Because elections are messy, difficult, and complicated exercises, risk is inherent in the administration of elections. While an expectation of perfection is unrealistic, we expect systems and measures to reduce or limit the level of imperfection as much as possible. Since we are unlikely ever to have perfect, risk-free voting systems, we advocate strongly for reliability and for independent auditability of elections to safeguard against many acknowledged risks.

a. *What are the essential elements of a risk assessment?*

Any reasonable risk assessment must determine the possible threats and approaches that might be used to eliminate or mitigate those threats. It should start by addressing the following points:

1. What security properties are being assessed (e.g., election theft, vote stealing; detection of inaccuracy vs. correctability of inaccuracy)?
2. Who are the potential attackers and what are their capabilities? For election systems, this set should include insiders with legitimate access to the software and hardware (and designs thereof), in addition to voters, poll workers, election officials, etc.
3. What is a baseline set of possible attacks that must be defended against?
4. What are the defenses?
5. Explicitly, what assumptions are being made about procedures?
6. Can we quantify the various risks, and if so, how?

Systems being analyzed should also include systems with ADA accommodations, to include threats that are enabled through the accessibility interface.

We urge the EAC to engage the technical community in general, along with the TGDC and NIST (both of whom have expertise in this area) to define a more precise framework along the above lines.

b. *How can the EAC best create a risk assessment that recognizes all possible risks and assesses the plausibility and nature of such risks?*

It is impossible for the EAC to recognize all possible risks, let alone assess the plausibility and nature of the risks. There is no question, however, that some voting equipment will malfunction in every election. The cause of the malfunction – equipment failure, poll worker error, Acts of God, or malicious attack – is secondary to the inevitability that malfunctions will occur. Consequently, it is unacceptable to employ voting systems that cannot recover from such malfunctions. And it is important to require that voting systems produce information that can help diagnose problems and prevent their reoccurrence in the future.

However, once a set of threats has been identified, criteria for comparison can be defined, following the framework outlined above. For example, a system that permits a very small group of individuals to change the outcome of an election should be considered riskier than a system that would require many participants and would have a much greater chance of detection.

c. *How do you evaluate what is an allowable level of risk?*

The allowable level of risk should be set at what can be feasibly and cost-effectively achieved with the best available equipment and election practices. In our opinion, the risk can be minimized using paper based systems such as precinct-count optical scan with careful and transparent manual auditing of election results, and optimal procedures for maintaining the integrity of the paper ballots between the close of the polls and the last recount.

2. *How can innovative systems be evaluated for purposes of certification?*
    a. *How can we create a certification process for innovative systems that isn't a backdoor around the standard certification process but at the same time isn't so cost prohibitive and restrictive that it presents a barrier and a disincentive to prospective inventors and manufacturers?*

We oppose creating a process that is so restrictive that it becomes a barrier to new inventors and manufacturers. However, there are certain conditions that must be satisfied by any voting system, whether it falls within the innovative class or currently established categories. Such a system must be secure, accurate, reliable, and have good usability and accessibility. It must protect the voter's privacy, and it must be easy to audit.

In order to satisfy the above conditions, any new system must be software independent and be based on an easily auditable independent voter-verifiable record (IVVR), for example a voter-marked paper ballot. It must also satisfy the testing requirements of current voting systems, including the six points listed in the response to question 1. In addition, it is critical to have public disclosure of those aspects of the system that are the basis for the evaluation. The public should know enough to be able to check the work of the expert evaluators.

    b. *Can a set of limited standards be created in order to make the path towards certification of innovative systems more clear? If so, how?*

We are opposed to creating a limited set of standards for certifying innovative systems. The reason for the standards is to make our voting systems as secure, reliable, etc. as possible. These are points on which there should be no compromise.

3. *What is the value of the open-ended vulnerability testing model?*
    a. *Are there any risks associated with this kind of testing?*

Open-ended vulnerability testing (OEVT), which is generally referred to as "exploratory" or "red team testing," is necessary to try to detect unanticipated vulnerabilities and hidden malicious code. Exploratory testing is widely recognized as a dominant testing method in most testing regimes.

OEVT testing should counteract some of the limitations of checklist-based testing and give more transparency and assessment of the quality of the vendor's own software process. If OEVT reports are made public, if we see that it takes the vendor several tries to pass OEVT, and if in the first few tries the testers find significant flaws, then we may have reason to suspect that the vendors' internal software design, engineering, and testing processes are deficient. The assumption might then be that what OEVT found is only the tip of the iceberg, and that the equipment reliability score should be downgraded accordingly.

However, OEVT is only as good as the testers. Doing OEVT well takes very highly skilled, expert testers. Testing by less skilled testers should still uncover flaws, and hopefully it will weed out the most egregious flaws. To ensure against inadequate or mediocre testing and in order to have accountability and transparency of testing labs, there should be disclosure of all source code and all other technical materials that the testing labs produce. If the testing labs do an inadequate job, then independent parties will have the access needed to do such an independent analysis of the testing labs themselves. Ideally, such independent analysis will keep the testing labs "on their toes."

EAC officials and all state election officials should have the authority to order an OEVT any time that they have concerns about the security of a voting system. The vendor should be required to fix flaws uncovered by the OEVT.[1]

b. What are the best ways to limit the cost of this kind of open ended non-scripted testing so that it can be useable within the EAC's testing program?

Cost should not be traded off for security, usability, reliability, accuracy, or accessibility. Voting is a matter of national security, and it should be treated as such. Nevertheless, there is a point at which the cost of testing will discourage the development of new systems. One of the primary reasons that we strongly advocate for SI, quality IVVR, and independent auditability is the understanding that they can potentially reduce the need to rely on security testing, compared with software-dependent systems.

OEVT should be based on clear criteria along the lines of the six points listed in response to questions 1. The testing should be searching for violations of specified security properties and making sure that there are effective defenses against specified baseline attacks. The findings should be evaluated in terms of well-defined risk metrics, such as the "number of informed participants."[2] In order not to restrict the choices of voting systems further, the OEVT policy should strike a balance between system quality and expense and delay.

c. If the EAC were to require OEVT how could it best be included into the EAC's Testing and Certification Program?

OEVT should be treated the same way as other tests. Vendors should be required to repair any flaws found in voting systems via OEVT.

4. Do methodologies exist to test voting system software so it can be reliably demonstrated to operate correctly?

There are no testing methodologies that exist that would allow us to know with certainty that a voting system will operate correctly and securely. This unfortunate fact stems from a fundamental mathematical theorem that shows that it is impossible in general to answer even

[1] Some states rescind state certification when unacceptable flaws are uncovered. A non-permanent certification could be considered at the federal level also.

[2] See *The Machinery of Democracy: Protecting Elections in an Electronic World*, a report produced by the Brennan Center for Justice at NY School of Law.

such a simple question as whether or not a software program will eventually halt.[3] One doesn't have to resort to mathematics to observe that software vendors regularly post patches to their software, in some cases years after the software was released, in response to emerging or previously undetected flaws or threats.

a. *If testing to a thorough set of standards is not enough to demonstrate the reliability of the system, what else can be done to improve confidence in electronic voting systems?*

The best way to improve confidence in electronic voting systems is to institute statistically significant random manual post-election audits of voter-verified paper ballots. Timely, accurate post-election auditing in turn requires getting detailed vote tabulation results quickly after polls close in an open standard format for the media and the general public, as well as for those responsible for conducting election audits.

5. *Throughout the creation of its draft VVSG, the EAC's Technical Guidelines Development Committee struggled to balance the need for useable and accessible systems with the desire to create the most secure system possible.*
   a. *How can the EAC best strike a balance between these sometimes competing needs?*

A well-designed system can be usable and accessible, as well as secure. Problems have arisen because a) some voting systems have not been well-designed and b) in several cases security, accessibility, and/or usability have been added on after the system was built. Ideally, all of the important features of voting systems can and should be integrated into the design and development of the systems from the beginning.

However, we also have to acknowledge some limitations of current technology. Quoting from email from Noel Runyan:

> Absolutely complete independence can never be obtained for all voters. For example, currently many voters with severe motor impairments and many blind voters cannot independently sign their own names in the poll books, but this does not mean that they cannot have enough independence to assure privacy of their ballot choices during other parts of their voting experience.
>
> With near-term technology, we should be making sure the voter has independence where it is essential for assuring privacy of the voter's ballot choices. As a goal, we should strive for 100% of voters being able to be 100% independent in their voting, but be willing to settle in the near term for systems that may require that a few voters accept some assistance that does not compromise the privacy of their ballots.

b. What level of usability or accessibility could be sacrificed in order to gain additional security or vice versa?

We do not believe that aspects of usability and accessibility need to be sacrificed for security. As with other aspects of the VVSG, we need to avoid creating requirements that are not currently

[3] This is known as the Halting Problem. The theorem is the work of Alan Turing, a renown mathematician who, among other things, broke the German code in WWII.

feasible for paper ballot based systems. Quoting from Noel Runyan's written testimony before a recent EAC round table:

> As currently worded, the measures required in the draft VVSG for assuring that voters with disabilities can have personal independence and privacy in their verification of paper vote records takes several quantum leaps in technology development. The draft VVSG goes unreasonably far overboard in apparently requiring that paper record verification for voters with disabilities and alternative language needs must carry out advanced OCR, autonomous ballot parsing and format extraction, and translation of languages other than English.
>
> This seemingly desirable super-verification system for voters with disabilities would require software and therefore not be software independent.
>
> Writing a requirement like this into the VVSG is somewhat like requiring a similarly desirable goal of converting all of our energy generation to fusion power plants within four years.
>
> These requirements for complete personal independence in paper ballot record verification are so technologically far into the future and impractical in the near term that the effect of requiring them in the VVSG would be to simply ban the use of paper ballot records systems.

6. *Are there any changes to the VVSG, in either scope or depth, which would significantly reduce the cost (time and/or expense) of compliance without adversely affecting the integrity of the VVSG or the systems that are derived from its implementation?*
    a. *What needs to be added or removed from this document to strengthen it and the systems to be constructed to its specification?*

We have a few specific comments and suggestions.

1) The EAC should consider expanding the definition of "voting system" to include electronic poll books, especially when they interface with voting systems. Ideally, standards, testing (including testing under Election Day type conditions), and certification criteria should also be applied to ePollbooks.

2) Many current VVPAT systems used with DRE's make voter verification and auditing difficult. Although such systems are better than DRE's without any kind of independent voter-verified records (IVVR), the new 2007 VVSG should require individual paper ballot records that are durable, easy for voters to read and verify, and easy to audit. The most cost-effective, fail-safe technology today is still a paper ballot that voters mark directly and which can be scanned immediately to check for over-votes, under-votes, and other marking problems. For voters with special needs, including visual impairment and languages other than English, the best supplementary technology is a ballot-marking device capable of producing paper ballots that can be independently scanned for voter verification and error checking.

3) We recommend that digital scanners, which should be defined in the VVSG and distinguished from optical scanners, be required to use a format with an open standard, to facilitate audits. the VVSG should distinguish between optical scan marksense scanners

and what are commonly referred to as "digital scan". These newer scanner make a digital image of the voter marked ballot and then interpret than image for tabulation. Standards for the accuracy and reliability of the initial image capture should be established and the image should be created in a loseless open format unencumbered by proprietary issues.The digital image, which the voter is not given the opportunity to verify, should not be construed to serve as an IVVR. We will provide specific suggestions for inclusion in the VVSG before the end of the comment period.

4) In order to support interoperability, as well as timely and effective reporting of results and auditing, all voting system components (including both hardware and software) should be required to support input and output of data using a standard open XML format. A currently available option is the XML-based Election Markup Language (EML) developed by OASIS.[4] The use of a standard XML format will make it easier to disseminate election results quickly to the media and the general public, as well as to those responsible for conducting election audits.

5) A problem with testing to benchmarks is that the software may be designed specifically to perform well for those benchmarks, as opposed to performing well in general. Ideally, there should be a sufficiently large and diverse set of benchmarks as to mitigate against benchmark driven code.

6) It would be desirable for optical scanners to provide descriptive messages when reporting an overvote or an undervote, ideally in multiple languages.

7) Poll worker usability of systems should be more precisely specified, e.g. ease of setting up, weight limits, complexity, limited amount of training time needed, etc.

8) Usability testing should simulate environments that closely resemble voting places, e.g. crowded, poorly lit, noisy, overheated, inadequate seating, etc.

9) Similar simulations should be used for accessibility testing, with the additional requirement to include people with a wide variety of disabilities in the group testing the voting system.

10) The notion of failure rate included in the VVSG is not ideal. Simply lumping all "failures" together in computing the failure rate can be misleading. Some failures might be critical, while others could be very minor.

[4] EML has been developed by OASIS over the past seven years, and is now being considered for adoption as an ISO standard. Recommended by the Council of Europe in 2004, EML has been used in different ways in a number of elections around the world, most recently by the California Secretary of State's Office to report statewide and county totals from the February 5, 2008 presidential primary elections.