United States Election Assistance Commission

Public Meeting

Election Official Roundtable Discussion

1225 New York Avenue, Suite 150

Washington, DC 20005

Held on Friday, April 25, 2008

VERBATIM TRANSCRIPT

Election Official Roundtable Participants List

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

Russ Ragsdale
City and County Clerk
Broomfield County, Colorado

Alice Miller
Executive Director, DC Board of Elections and Ethics
Washington, D.C.

Paul Miller
Technical Service Manager
Washington Secretary of State Office

George Gilbert
Director of Elections
Guilford County, North Carolina

Lowell Finley
Deputy Secretary of State for Voting Systems Technology & Policy
California

David Drury
Bureau Chief, Voting System Certification, Florida Depart of State, Division of Electronics

Keith Cunningham
Director, Board of Elections
Allen County, Ohio

Deb Seiler
Registrar of Voters
San Diego, California

Mark Skall
Software and Diagnostics and Conformance Testing Division
National Institute of Standards and Technology

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

PUBLIC MEETING

ELECTION OFFICIAL ROUNDTABLE DISCUSSION

DR. KING:

This morning we have a roundtable discussion scheduled from 9:00 until 2:00 p.m. We'll take a one-hour break at lunch. There's an important metric in this. There are ten panelists, six questions, and three hours of discussion. And I ask everybody to self regulate so that to date we have finished all of our roundtables in a timely fashion and my hope is that we will do the same today. I'd like to first recognize Commissioner Donetta Davidson joining us this morning, thank you. And since we only have one other person in the audience, I think I'll recognize the whole audience. Good morning, Carol Burkett.

MS. BURKETT:

Good morning, glad to be here.

DR. KING:

For those of you that don't know Carol Burkett - and we have a format to these roundtable discussions. We've essentially worked with the same six questions with a variety of panels over the past four months and it's been insightful. Everyone has yielded additional information and additional viewpoints, but to begin with this morning what I'd like to do is start here with Keith and we'll go around the table and if you would introduce yourself and the organization that you represent and your role within that organization. Go ahead.

MR. CUNNINGHAM:

My name is Keith Cunningham. I am the Director of the Allen County Board of Elections. The county seat is Lima, Ohio, northwestern part of the state. County of 512,000 people, 70,000 registered voters. We run and have run since 1995 a precinct count optical scan operation with the Automark says the handicap component. Go Buckeyes.

DR. KING:

Okay, thank you, Keith. And as we go around the table there's two microphones that are distributed, there's two sets of microphones. There's actually three different kinds of microphones. The microphone with the cable is going to the transcriptionist here and they're very sensitive, you don't need to move them around the table. The microphones for the room are these cordless microphones and the little flat black cordless microphones. So if you can make sure that one of those microphones, one of the house microphones are nearby when you speak.

I'd like to also recognize Commissioner Rosemary Rodriguez has joined us this morning. Good morning Commissioner and Executive Director, Tom Wilkey has come in. Good morning, Tom. It's David.

MR. DRURY:

Okay. My name is David Drury. I'm the Bureau Chief for Voting System Certification, Florida Department of State Division of Elections. That's basically it and I'm trying to keep out of trouble.

DR. KING:

Good luck with it. Lowell?

MR. FINELY:

I am Lowell Finely, not Finely. This is just for everybody's benefit as you're referring to me, just get my name right. I am the Deputy Secretary of State for California for Voting Systems Technology and Policy.

DR. KING:

Thank you, Lowell. George?

MR. GILBERT:

I am George Gilbert. I'm Director of Elections in Guilford County, North Carolina, a jurisdiction of about 330,000 registered voters. We are a DRE county and have been for the entire 20 years of my tenure there.

DR. KING:

Thank you, George. Paul?

MR. MILLER:

Paul Miller. I'm with the Washington Secretary of State's Office, Technical Services Manager. And one of my responsibilities there are the certification of voting systems for the State of Washington. And before that, I was Assistant Director of Elections in King County.

DR. KING:

Good. Alice?

MS. MILLER:

Good morning, Alice Miller, Executive Director for the D.C. Board of Elections and Ethics. We have a dual system. We have both the optical scan and the DRE that we have been doing about I guess for the past two and a half three years and registered voters about 400,000.

DR. KING:

Thank you. Russ?

MR. RAGSDALE:

I'm Russ Ragsdale, the City and County Clerk for the City and County of Broomfield, Colorado. We're a small jurisdiction of 25,000 active registered voters. We operate vote centers. We use the Premier System, primarily precinct based optical scan with the touch screen accessibility devices. We are small in population but large in decibels.

DR. KING:

Thank you, Russ.

MS. SEILER:

I'm Debra Seiler. I'm theThank Registrar of Voters for San Diego, California. And San Diego is the third largest jurisdiction in California. We have 1.3 million registered voters. For this coming election, we will have 1,652 precincts that we manage. We have been a DRE county, however, in light of the Secretary of State's decertification and recertification, we have gone to for the last February election, we went to using our precinct scanners in a central count environment so we brought our paper ballots back and we counted them centrally. We put one touch screen in every polling place to comply with HAVA.

My background is in both the Secretary of State's Office and the private sector a former member of our state's Fair Political Practices Commission and came to San Diego from Solano County which is the Bay Area where we used the ES&S System with a precinct count optical scan and the Automark.

DR. KING:

Okay, thank you, Deb. Mark?

MR. SKALL:

I am Mark Skall from NIST, National Institute of Standards of Technology. We have a long history of developing standards in various areas of IT on development tests and we of course we were brought into this rather fascinating area by HAVA in 2002 and we're glad to help and we are from the government and we are public servants.

MR. HANCOCK:

Here to help.

DR. KING:

Thank you, Mark. Brian?

MR. HANCOCK:

Thank you, Merle. Brian Hancock, Director of Certification for the Election Assistance Commission. And on behalf of our four commissioners and our executive director, I do want to welcome you here today and thank you all for joining us. We know that 2008 is an extremely busy presidential election year and we know your schedules and probably more than any of the other groups you guys are pressed for time and so please know that we do appreciate your taking time out to help us in this really important project.

This is the sixth of the roundtable discussions that we've had. It seems like they've been going on for quite awhile. Mark and I have been in this exact same position staring each other in the face for all six of them. And I think they have all been good. In each one of them, we've had different groups, different participants in the process, and they've all shared with us information that I think we can take back and information our commissioners can use to make more informed decisions when we get to the point of finally adopting this document.

I just want to remind you of a few things. Because of the extended nature of these roundtables, we also extended the initial public comment period for the VVSG and the close of that public comment period is now May 5. So those of you that have not put comments in and wish to, please remember that date. We would love comments from everyone. And certainly since these are going to be affecting you all to a great degree, I think it would behoove you to comment as you feel you're able to.

You know, certainly one of the important things we want to lay out here is that this next iteration of the VVSG is really going to chart the course for the development of election officials, of voting systems for election officials and to the foreseeable future. It's certainly not our intention to continue to go through a standards development process every two or three or four years. That doesn't serve anybody's purpose so we want to make this document the best document that we can in conjunction with our partners at NIST and the TGDC to make it viable for quite some period of time.

So remember, we're looking to the future with this document. And again, we certainly realize that this future has to be married not only to technology but to election administration practices. And to that end, you know, while we're concentrating right now today on the VVSG, most of you are also aware of our program for developing election management guidelines. We think those are very useful and we've gotten particularly from county officials a lot of good responses to those and I think it's important to realize that that's not sort of talk down thing. It's not the federal government dictating. The information we're getting is actually from working groups of state and local election officials. Some of you here at this table, in fact, George and maybe a few others, I think Alice have been at those working groups and provided valuable input so we're looking at both aspects because we know the machines even though they're an important part, they're only a small part of the system and without the procedures, the machines really don't mean a whole heck of a lot.

So with that, I'm going to turn it back over to our moderator. But before I do that, I want to thank Matt. Once again, he's done the majority of work for putting these roundtables on and to the event, to the extent that they're a success; he's responsible for that. So thank you, Matt.

DR. KING:

Okay, thank you, Brian. A couple of housekeeping items before we begin the discussion. If you have cell phones or PDA's or anything else that needs to be silenced PC speakers, music, now's the time to do that.

As I mentioned earlier, we have six questions that we want to address before we break for lunch today at noon. We'll also take a break at about 10:30 and so I'm hoping that we can explore every dimension of the question that we can in that period of time but it is important that we do keep on schedule. When we come back from lunch at 1:00, each member of the panel will be given an opportunity to kind of summarize what they think is most important and most salient for the EAC to take away from this discussion today from their perspective or their jurisdiction or from their perspective as an election official in a larger context. At that closing summary period, we'll take about five minutes each as we go around the table. So if we don't get a chance to explore the questions, the six questions at the detail level that you want there's still an opportunity for you to come back after lunch and make the points that you consider really need to be evaluated by the EAC in this context.

As Brian mentioned, this is the sixth roundtable discussion that we've had. We have completed roundtable discussions with security experts, with voting system manufacturers, with voting system test labs, with usability and accessibility experts, and with voting advocate groups. And today I think is an important watershed day in this series because at the table I think are obviously the people where all of this gets traction. All of the work of the VVSG which is in a sense transitory to the construction of systems, it gets implemented by the people around the table. So the buck stops in many cases with the folks at this table. So I'm personally looking forward to the perspective of the election officials as we begin this discussion.

Each of the topics that we'll discuss will have a brief introduction and I think Lowell, you volunteered to introduce

Question #4. And I will take a shot at introducing the other questions.

So Matt, if we could bring up the first question if it's not already up here. The VVSG has many stakeholders. And at first blush, I think it's easy to construe that if the document was written for manufacturers, it was written for the testing labs. And so the question that's evolved over the prior discussion panels is how do the other stakeholders and certainly election officials are stakeholders, voters are stakeholders in this process, but how do the election officials look at the issues brought forth in the VVSG? So the question here is the VVSG has more than one audience including vendors and VSTL's. Do you consider county and state election officials as one of the stakeholders and therefore one of the intended audiences of the document? And if so, is the document in the whole or in parts intelligible to the election official community? Can it be read? Can it be understood at face value and can the implications of its implementation be understood by election officials? And then most importantly, the following question how can it be improved from the perspective of the election official?

So with that introduction, I'll open it to discussion. I'd ask for one rule. If you'd like to be recognized, if you could put your name tent up on end, that helps me keep track of who wants to talk next and we'll work through the people in the order that the tents go up. Alice, thank you, good start. Alice, and then Deb, and then Lowell.

MS. MILLER:

I think that parts of it are more intelligible than others. Obviously it's a technical document so it's written to technical standards and I think that has to be taken into consideration when you start reviewing this process. There are parts of it like the human factors part of it is easier to understand than the security and transparency part of it at least from my perspective.

And having sat through many of these hearings regarding the development of this document, I can tell you that it was hard for me to follow a lot of it, but I understand that it needs to have the technical balance because it's done to standards. I wouldn't expect anyone for example to be necessarily able to easily read a legal document if they hadn't been legally trained. They may understand it but it may just take a little bit more time for them to analyze it.

With respect to how it can be improved, I think you've just got to review your processes and change what can be changed.

DR. KING:

Okay. Deb, and then Lowell, and then George.

MS. SEILER:

Thank you. Well I guess I would echo what Alice just said in terms of it being understandably and necessarily I'm sure a technical document. I think that that's appropriate and clearly the document itself states that it's intended for manufacturers and the test laboratories and so -- but election officials, I believe are a crucial audience because everything that happens as part of this process will come home to roost with us. I mean this is really as you said this is sort of where the rubber meets that road.

And I think it's a difficult daunting document for most election officials to get into. I think it would be helpful and maybe it's too late because it's obviously close to the end of the comment period but to provide some sort of seminars or something for election officials to begin to understand the document, to put it into a certain context, and be able to follow it. After you work with the document for several hours and go through it and go through the introductory portions and then start wading into the technicalities, some of it can become clear. Some of it is engineering standards, which of course are never going to be that intelligible to election officials. But I think what would be helpful would be some sort of introductory seminar kind of presentation to help election officials comprehend it, combined with perhaps a document much shorter in length that might be 50 pages, even 100 pages that would sort of layout in much more lay terms what the effect would be. And then I think election officials would feel more comfortable sort of wading into it. Of course setting aside the things that they know, you know, meantime between failure or some other engineering term that, you know, we understand we're probably not going to have any expertise in. But I think it's important for us to have an understanding of how this is going to impact us. And some of these things are laid out in the document. I didn't walk away with it in all cases with a real understanding how is this going -- what practical effect is this going to have on my operation? And what management tools do I need to be able to cope with this?

DR. KING:

Okay, thank you. Lowell and then George?

MR. FINELY:

I look at it from the point of view of a state election official and in state where by statue we can only approve systems that have been certified at the federal level but the Secretary of State has independent authority to decide whether or not to certify systems even when they've been approved at the federal level. So from our standpoint, I think that state officials are definitely an intended audience or an important audience for these standards because we're watching to see and hoping to influence how robust these standards are and how robust the testing system is as it rolls out.

We would like to be able to place much greater reliance on federal standards and on federal testing and not have to spend as much time and as much money on separate state testing that takes place after the federal process has finished because that clearly has cost both in times with in terms of time and money. But if, you know, a state of our size and with the capacity to do some independent testing is not satisfied that these are sufficient standards then we have to consider going our own way or continuing to do that.

And with all that said, I think the standards, the guidelines have been drafted in a very clear way that's very useful to us. We have the luxury of being able to spend more time and devote more people to analyzing it than most local officials would do and I certainly recognize that. But I think it is a very user-friendly document given what everyone else has said about the fact that it involves engineering and computer software development issues. So I commend the people at NIST and the TGDC and others who have been involved in putting it together.

DR. KING:

Okay, thank you. George, and the Paul, and then Mark. George?

MR. GILBERT:

Local election officials are the ones who use voting systems. We are the ones who deliver the service to the voters. We are the key and the linchpin in the whole operation. Everything you do in technical standards affects not just the operation of the equipment, but it affects our management processes, our business processes, the cost that we have to go to our counties or states and implement.

Ultimately the security of elections in my view is going to depend on the people that are implementing those elections. You cannot build a fail-safe voting system. You never will be able to. What we need is reliable voting systems that can be efficiently deployed using good management. Elections are as much about management practices as they are technology. And to design technology in the vacuum will create I think results that will be devastating to the entire process.

As Deb pointed out, we need to know what the implications of these standards are. When I read the standards after awhile, I can figure them out. Then when I read the vendors comments on the standards of what they say the implications of this is, I get a very different picture than what's presented in the standards. If the states, the counties, the vendors, if the EAC doesn't know what the implications of these standards are going to be, I don't see how you can proceed.

So I think we've got a long way to go. The document that we have out there now is unintelligible to 95, 99 percent of the election officials. Not because they aren't intelligent enough to read it and understand it, but there's no way they're going to read it. They're not going to be able to read the entire document. We're burping a baby here that's going to have major implications for all us for a long time and no pun intended but I don't want it to be Rosemary's baby in the traditional sense, nothing personal Rosemary. literary Rosemary's baby. That's a -- you'll hear that theme again.

DR. KING:

Can we count on that, George?

MR. GILBERT:

You can count on it.

DR. KING:

Thank you. I have Paul, and then Mark, and then Russ. Paul?

MR. MILLER:

One thing that I think both Alice and I failed to mention is that we were on the TDGC that was part of the committee that drafted the standards. And time and again one of the issues that we had to deal with was that we can't and should not be putting procedures into the VVSG. But what that does mean is that there needs to be some sort of translation, something that says this is what the implications are procedurally for elections, for the local election officials and I don't think that's in place.

DR. KING:

Okay, thank you. I've got Mark, and then Russ, and then Keith.

MR. SKALL:

Thank you. There are many stakeholders in this process. Clearly election officials are major stakeholders. The way standards are written is they are written containing requirements, mandatory requirements that need to be implemented. This particular standard is written to be implemented by two sets of equal manufacturers and test labs. There are specific requirements that pertain to them. Thus there has to be specific, precise language that tells them exactly what to do. That's a necessary but not sufficient condition for this whole community. If we don't have that, we don't have the system that's going to be secure and reliable. So that's a necessary condition.

There is sometimes an inherent conflict between precision and readability. I wish I had a magic bullet to say, you know, we have to tell people exactly what to do and we have some formulas and make that readable. We did hire a readability expert to help us write this. We looked at every section and tried to make it as usable as possible, but the bottom line is it has to be precise.

As far as the implications that you brought up, George, I think we have to all understand the implications and we do that by dialogue. We cannot -- a standard is not written to be a long narrative about various implications. It's written to document requirements but I think we do have to understand the implications.

And I think Deb made a great suggestion and you almost seemed like you were shield and put here just for this because we did have a seminar for voting officials to train them in Boulder, Colorado. We are, I don't know how many of you were there some of you, I think. And we are making that available by video for people to look at. We have a companion document as well so thank you for that, about a 50-page document that summarizes the requirements. Again, it is not a normative document. It helps explain things. When you want to find the actual requirements, you need to go back to the standards.

So it's a complicated process, we're certainly aware and we try to make things as usable as possible but I wanted to point out there is a need for precision and there's no getting away from that in the standard.

DR. KING:

Okay, thank you. Russ, then Keith, then David.

MR. RAGSDALE:

Excuse me. I'd like to expand on that. I did have an opportunity attend that Boulder training and Mr. Skall's absolutely correct. It was a great insight for me to see the intricacies. Obviously the VVSG is a purpose document and it's not a user's manual for election officials. It was never intended to be. I know the EAC Standards Board and Advisory Board had requested the NIST to develop the companion document. And Mark, maybe you can help me out, that there was a draft with some limited release at the Austin conference in December. Where is that now?

MR. SKALL:

I think we are actually going through our process through our editorial review board to get it final and make it distributable.

MR. RAGSDALE:

Great. Well I think that's critical that we have a document like that because not only for the use of the systems that are developed to the VVSG standards but for the procurement of the systems. Bear with me here. I'm thinking of the county on the eastern plains in Colorado and the clerk and recorder and I'm appearing in front of my county commissioners and I'm asking to buy ten voting booths, electronic voting booths that are built to VVSG specifications. I need to be able to understand to be able to convince my -- the budget people why that system has the characteristics it has and the price tag it carries. Right, wrong, or indifferent, that's still my job, before I ever get to use it or to try to train my voters on how to use that system. So I think that's something to keep in mind, too.

DR. KING:

Okay, good, thank you. Keith and then David.

MR. CUNNINGHAM:

I was at the Boulder event. What a mind numbing experience that was. Wow. Yeah, I guess, you know, I drive a car every day and I -- but I have no idea how it operates. I take it for granted that the people who develop the standards for the automobile and the people that manufacture the automobile have communicated on that and everything's good.

I don't know that it is important that a local election official understand about 80 or 90 percent of this document. I think that you're right it's purpose driven standards document. It has to be specific. The problem is that the standard then creates an expectation on the election official for some type of procedure or the ability to deliver some type of an answer to a question. And there, I think is where the, you know, where we've got to create the connection. I think whether it's the document that the Advisory Board talked about, a plain spoken, if you will, companion document.

But I think, you know, what I'm focused on as I've looked at this because I, you know, I'll be honest with you as if it's a big secret I don't know the first thing about cryptology. I probably wouldn't be doing this if I did. I'd be, you know, working at NIST or something.

MR. SKALL:

And making big bucks.

MR. CUNNINGHAM:

Yeah, right. But I look at the usability and the functionality sections and I think there is where we have to again go back, you know, the standards create an expectation on the local official to deliver certain things in the way of security and use and results and so forth. And whatever we can do, I don't know if it's a companion document. I don't know if it's a rewrite of some portions of this that, you know, in a companion document or what but that to me is where we're all struggling. Is how do we connect between the extremely technical that there are certainly other people to take care of and then the end result which is the usability and functionality on election day.

DR. KING:

Okay, thank you, Keith. David?

MR. DRURY:

Well everyone is pretty much in agreement to the stakeholders. From my perspective from the state aspect, we will do whatever we need to do. From the jurisdictional point of view, from the counties it's a problem with customer wants. That's what they really want, the customer wants. But that's a full spectrum, full spectrum meaning a large county like Miami Dade 750 plus precincts all the way down to Lafayette, which is 500 precincts. Miami Dade wants to see what we can do to change it. Lafayette will say please don't change anything that is going to cost me. The whole idea here is the cost. That's a real issue.

DR. KING:

Okay, thank you, David. George?

MR. GILBERT:

Merle, I'd like to address a specific, I mean maybe an example of the kind of thing that I'm concerned about which I included in my written remarks. You've got a standard that addresses privacy for the voter and it's a fairly absolute standard. It basically says that the voting system cannot associate a voter with the ballot except if they're a provisional voter. Well that doesn't meet North Carolina law. You've got to know what the laws are out there before you go writing a standard for the equipment that can be used in those laws. And right now that this document goes far beyond in my view, it makes assumptions about what the standards should address. What the performance standards should be. And the performance standard is based on what state law is requiring.

So I think a lot of things in here like that. I included a lot of those types of examples in my written comments on the VVSG. But there are more than one example and those are the kinds of implications that I'm talking about. Yeah, you have a standard that's very clear and it has to be clear to the vendor, but it doesn't work for us. Thank you.

DR. KING:

Okay, good. Keith and make sure you put that sign up, okay.

MR. CUNNINGHAM:

I actually just have a question.

DR. KING:

Okay.

MR. CUNNINGHAM:

George, I'll just give you a perfect example of that and this goes back to what I was saying. These standards discuss the notice of an under vote. Well then that creates an expectation that we will notify people of under votes. Well the fact is in optical scanning at the precinct level, notification of under vote A, slows the process down dramatically. And B exposes the voter to other people knowing that they didn't vote their entire ballot. I have a lot of complaints coming from voters that say whose business is it that I decided not to vote for the Supreme Court Justice? So the standard creates an expectation that is certainly not a practical expectation when it comes to, you know, the fundamental application on Election Day.

An excellent -- Dave had mentioned the cost. I just probably want to get this on the record more than anything. I think that it's time we start to begin to look at the cost. We're spending, the amount of money we're spending running campaigns versus the amount of money we're spending actually conducting the election and I think we'll get some very revealing numbers that we're way out of balance here. And, you know, we -- let's make that dollar check off on your tax return for election administration and not political campaigns.

DR. KING:

That’s a great idea.

MR. CUNNINGHAM:

Commentary, sorry.

DR. KING:

Let’s get Lowell and then Mark.

MR. FINELY:

I just had a question concerning North Carolina Law. Does your state require systems to qualify under federal standards in order for them to be used or is that optional?

MR. CUNNINGHAM:

Optional, but optional only technically because the minute you go out and deploy a system that doesn’t have federal certification then all the people that, you know, want -- then you end up in a huge public relations problem. So I mean, we call these VVSG’s but, you know, they’re really not voluntary anymore on any state so as a practical matter they’re mandatory.

DR. KING:

Okay, thank you. Mark and then Paul.

MR. SKALL:

Okay, thank you. Well clearly I think if there are any requirements in the VVSG that violate any state laws we’d like to know about them and further comment, but I’m sure the EAC would as well. But I guess I’m little confused because the example that Keith gave or provided talked about these are requirements for voting systems and they’re typically worded that the equipment shall have the capability to do something. That doesn’t mean you have to use it.

And I guess your argument is if it has the capability we are creating an expectation it will be used. I mean that's a political issue, that's not a technical issue but certainly if we took the intersection of all these negative requirements in states, we couldn't have anything in the standard. Different states have different things so what we're doing is sort of looking at the union and saying they shall have these capabilities. It doesn't mean each particular state is going to use these capabilities.

So I'm not sure if that answers your concerns but I was talking about Keith's question. Certainly if we do something that's mandatory that's going to violate something, then that's something clearly I would think the EAC would want to fix. But just because you have a capability, doesn't necessarily mean one has to use that capability and the discretion is on the jurisdiction.

DR. KING:

Okay. Paul and then George.

MR. MILLER:

Yeah, I was going to follow up on Mark's comment but actually I originally put this up to say almost exactly what Mark said. But to -- in terms of response to Keith, it's my understanding that all the voting systems currently have the capability already have the capability of rejecting ballots for under votes. In fact, I don't think that's -- I think -- I don't believe that that's a new standard. And so it's been there all along.

DR. KING:

Okay, George.

MR. GILBERT:

I read the VVSG with that perspective in mind and in my comments made note where I thought the language of the standard as written was permissive and where it was mandatory. In the case that I'm referring to, it did not appear to be permissive; it appeared to be mandatory. And I have heard the same argument made with respect to Keith's issue. So it may be simply a matter of cleaning up the language a little bit. Clearly what you're suggesting should be a capability of the system, but not mandatory.

DR. KING:

Okay. I wanted to follow up with a couple of questions to the panelists. And Alice, when we had the usability and accessibility roundtable, I think we heard the expression plain language probably a dozen times in that roundtable. And when you said that there were parts of the VVSG, the human factors for example that was easier to understand than say the security is that a reflection of the inherent complexity of those sections or on your background and your familiarity? I guess if we were to move forward with a recommendation as a result of this roundtable because we heard from Deb that training is an issue. So the question is do we need to bring election officials understanding up or do we need to create greater clarity in some of the sections of the manual?

MS. MILLER:

I think it's clarity in the sections of the manual. Secure -- I'm not technical and I say that to my staff all the time. I'm the least technical person that there is. It's just that simple, but I can follow the processes. Reading this and trying to understand some of the security parts of this I will say was very difficult because it is very technical. So I don’t know you, you know, take the technical out and make it plain language because again, I understand what Mark’s point is.

DR. KING:

Um-hum.

MS. MILLER:

It’s a standard and it has to be written to the standard.

DR. KING:

Um-hum.

MS. MILLER:

And tested to the standard and the standard have certain components in order to make it work. On the other hand, it still does not negate the fact that it’s difficult to follow. So maybe the companion piece, you know, would help with that. So I think you need to change the language as opposed to bringing the official’s level up because I think the most election officials, you know, have a good sense of what they’re doing and they know to do it, but trying to understand this document is a whole other issue.

DR. KING:

Okay, good. Deb?

MS. SEILER:

Yeah, I just would like to well thank Mark for pointing out the fact that apparently a video does exist and a companion document does exist. I was unaware of that. I don’t know how many other election officials were aware of that. I would make sort of plea for greater education among the election official community.

DR. KING:

Um-hum.

MS. SEILER:

We for example in San Diego County have three elections coming up in the next 39 days. So our, you know, just -- and we have been conducting elections almost continuously since last September.

DR. KING:

Um-hum.

MS. SEILER:

So small ones certainly but, I mean, when we -- I actually was part of the first standards group back in the 80's and that review process occurred over a period of about four years, four to six years as I recall. I know that we don't have the luxury of that kind of time. And I know that there are real needs. But I would just like to say that if I had my druthers, I would like to see this go into a time period when more election officials could look at and have the opportunity to be educated and to educate themselves.

DR. KING:

Um-hum. George and then Brian.

MR. GILBERT:

Keith mentioned earlier that he didn't know how important it was for election officials to understand these standards and I agree 100 percent with that. The purpose of educating election officials about the standards is so that we can educate you about them. You're going to write the standards. The EAC is going to approve the standards. A political understanding is on your behalf that you know what the implications are when you write the standards. You've got to have a much deeper level of knowledge about elections then you have. We don't have to have a deeper level about technology but the deeper our level about -- of understanding there, the better we can communicate to you what the implications are for the application of this equipment out in the field.

So it's, you know, the fact that you're having these roundtables is a major part of this, you know, with this process and that hopefully it will help you understand what our concerns are, why we have those concerns, what the implications are, and how those feedback into the standards that you write.

DR. KING:

Okay, thank you. Brian and then Keith.

MR. HANCOCK:

Thanks, Merle. I just wanted to speak to the educational portion here. And I think I agree with you. There are sort of several levels of educational effort that we need to put forth. I mean I think this is part of the initial effort, the roundtables, the seminar that NIST put on, you know, that is web cast, and the companion document. And that's sort of the first part of the effort to try and educate people about the Draft VVSG. You know, what's out there now is not going to be the final document. When we get to the point of having a final document, you know, I would suspect the EAC staff will recommend to our commissioners that we do exactly what you're suggesting, that we have some sort of concerted effort to train election officials on what that final document is and as much as we can on the implications of it. I think the implications are going to be different from state to state depending on your state law so one of the other things you may want to look into may be in concert with

NASAD or some other election official group as to help them help us understand what the implications are from the various states. And to that end, maybe regional meetings might be helpful and sort of save on budget a little bit, too. But we're aware of it and I think we'll be addressing that issue.

DR. KING:

Thank you, Brian. Keith?

MR. CUNNINGHAM:

I just realized something that Mark you said. There's politics in all of this. Gosh, it reminds me of my favorite seen in Casablanca where Humphrey Bogart says there's gambling here? There's gambling here? And there lies the problem. And yeah, Paul I know that's an old standard. My point is that these are going to be heavily scrutinized and they are going to be used by, you know, political entities, political figures. Let's face it we have different goals in this than the politicians do. And they're going to be looking for advantage. And we've just got to be careful that we do not create expectations and unintended consequences trying to deal in such a pure environment that we're dealing just with the standard and don't take into consideration that no matter what it is on election day it comes down to people and it comes down to the voter and the election officials and so on and so forth.

DR. KING:

Thank you.

MR. CUNNINGHAM:

It's not technical on Election Day I guess is my point.

DR. KING:

Okay. Keith, I wanted follow up on something that you said earlier about and I'm paraphrasing here, but what does an election official need to know about the VVSG and why do they need to know it? And I wanted to put out a scenario for discussion of the group, which is explaining to individuals, or groups why a system that's selected in your state meets the VVSG standard but may not meet the voter's expectations. And whether that creates a scenario that raises the need for election officials to really understand what's in the VVSG.

MR. CUNNINGHAM:

Are you directing that a me?

DR. KING:

Yes.

MR. CUNNINGHAM:

Well obviously the -- I believe the election official or I wouldn't be here if I didn't think the election official didn't need to know it enough to discuss it in some intelligent way and engage in a -- the ability to explain to the voter in a satisfactory way why it isn't meeting their -- why it doesn't do what you think it should do. I mean we all know that everybody's got an opinion about how we should be voting. And, you know, you find yourself in whether it's before the rotary club or just in a group of people and when you explain to people why, you know, that bizarre concept might not work, they suddenly oh, yeah, okay, that makes sense, you know.

So but again, I don't think that in order to effectively operate and deploy a machine you need to understand the cryptography involved in it. You know, but you need to know that cryptography goes in here and comes out here and somewhere in the middle it gets jumbled up. But I think it's unrealistic. And I don't mean this in a negative way. I think it's unrealistic to think that on a large scale the election officials across the United States are going to fully digest or understand this document given the wide vast, you know, different circumstances there are.

DR. KING:

As I heard the first part of this discussion this morning, I was reflecting on something that we heard at the very first roundtable from Ron Robess [ph] and he had a very eloquent description of what voting standard should consist of and I think it was cast as intended, collect as cast, and count as collected. And I thought that would be great if we had a three line one stanza of voting system standard to review.

Okay, any other discussion on this topic? Okay, if not, Matt, could we move onto Question #2 which is in risk assessment. Risk can be described as a threat to the continuity of a system. Systems are designed to accomplish specific goals and risks are those things that have the potential to disrupt a system or subvert the system so that those goals are not accomplished. Often when we hear discussions of risk to voting systems, they're painted with a very broad brush and often wrapped around phrases like the integrity of the vote. And often it's a challenge to think about how could we assess that particular risk in the context of a larger risk assessment document.

In commercial systems, we often will look at the probability of an event occurring and multiply it by the consequence, the dollar consequence of that event occurring, and we use that as a way to prioritize risk and then as a follow on to prioritize how we're going to expend our funds to mitigate those risks. And even though there has been some work done on risk assessment, there's not been a complete published risk assessment for voting systems that could be a part of this VVSG process. The key as we look down the road as we listen in these roundtable discussions is without a consensus risk assessment document, it's very hard to reach a consensus on the inherent tradeoffs. And some of the tradeoffs that we've heard discussed is trading off accessibility for security. That's a common one as an example that's come forward.

So the question as it's posed here, it's up behind me now, NIST did sponsor a workshop in 2005 called the Risk Assessment Workshop. And there was an excellent start and the EAC is now interested in learning how to best develop a risk assessment framework to provide context for evaluating security implications of using various technologies. The question is what are the essential elements of a risk assessment of voting systems? Probably we could not identify all of them at this table but from an election official perspective what are the most salient elements of risk? How can the EAC best implement a process to create a risk assessment that recognizes the possible risk and assesses the plausibility and the nature of the risk? And then begging the question, if we cannot audit all risk out of a system, what is an acceptable level of risk?

So if we can start then with the first of the questions, what are some of the essential elements from an election official's perspective of risk in voting systems? Okay, Deb?

MS. SEILER:

Well I think any risk assessment from an election official's perspective is looking at the totality of the circumstances of your election. I mean it's not only who's going to maybe hack into your DRE or your optical scanner or whatever, it's really about what kinds of problems could you encounter. I mean our, in our last election for example, we were literally guessing at the number of paper ballots that we needed to order. We have non-partisan cross over voting. We have provisional voting that allows people to go into any polling place and cast a ballot, which we have to remake. In one case, we had more visiting provisional voters in a precinct than we had registered voters total. More people came into that place to vote than we had registered.

So those are -- that's I think a risk to a system and to your whole election day process that needs to be factored into this. And I don't really see it. I don't know how -- it's not something you could probably -- that NIST could write a standard for but I think it's certainly a consideration when you're looking at the types of voting systems you deploy.

DR. KING:

Um-hum. So many of the risks are behavioral oriented as opposed to inherent...

MS. SEILER:

Yeah.

DR. KING:

...technological issues, okay. George and then Russ.

MR. GILBERT:

Well I guess that was my point. I agree with Deb 100 percent is as election officials, as precinct officials, as workers in the election process, we are capable of creating threats that you can't even imagine and we do it all the time, I'm sure. There's been some talk about -- I mean, the standards talk about a risk assessment team, blah, blah, blah. The first thing you need to do with that team is send them out to our jurisdictions for about six months while we're preparing for an election and let them watch all the crazy things that we do. If you want to find out what the actual threats are to an election, you need to be there and see what is actually taking place. How this technology is in fact used in the voting environment. You know, the preparation for the election, the physical security issues, the management processes that go on. What can a precinct official do at the polling place? They can do amazing things.

So I think that that's the first step because once again you've got to know how this technology is applied in the field in order to be able to assess the risk to it.

DR. KING:

Okay, thank you. I've got Russ and then Lowell.

MR. RAGSDALE:

I've been able to do some reading at the workshop that NIST held on risk assessments and one of the things that I noticed in there was identification of cost. There was identification of the cost of the -- mounting the threat to help determine the plausibility. There was identification of the cost that if that threat or that risk takes place, you know, what is the damage? But what it seemed missing was the cost of mitigating that risk. Unfortunately, as an election administrator, I have a limited source, limited pool of resources. That's an element I would need in a risk assessment is what's it going to cost me of time, money, staff, what have you to address that risk? It could be a great deal of damage potentially from that risk but again, connect it with the plausibility and does that compel me to devote a significant part of my resources to mitigate that risk. So I would ask if any effort is made at a formal risk analysis that that's a component that's emphasized.

DR. KING:

Okay, thank you. Lowell and then Paul.

MR. FINELY:

I think risk assessment as it's been proposed for study in the document that the commission has put out is something that we need to recognize from the outset involves a great deal of subjectivity and speculation. And I think that's important because otherwise I think we can mislead ourselves into believing that if we conduct a multidisciplinary study that, you know, lasts a year and a half, we will have very precise metric a the end of it. The problem is that there are critical elements in risk assessments determining the probability that a particular vulnerability might be exploited and determining the level of harm that could result from it that are extremely difficult to actually predict or quantify.

And I think we've seen that a good example of it in which, I think a very serious attempt was made was the Compuware [ph] study that was commissioned by the State of Ohio in 2003 of the systems that the state was employing at that time. If you look at that document, it assigns levels of probability to various risks and it assigns levels of harm, but if you try to look behind that it’s very hard to determine how those were arrived at.

I think risk assessment is valuable in terms of classifying the different risks that exist and the consequences of there being triggered or being exploited so that you know whether you’re talking about something that changes the outcome of an election, that prevents the election from being conducted, that makes auditing difficult, that falsely creates the impression that there are discrepancies. There are lots of different kinds of things that can go wrong. And so I think that’s valuable.

But I’m concerned that the proposal to conduct a very long-term risk assessment when it’s framed as something that needs to be completed before the commission and the VVSG can arrive at meaningful standards, threatens to delay the implementation of serious security standards in particular. And if the entire VVSG is going to be held back while we wait for that to be completed, then I think we’re talking about stretching this process out to the point where we’re looking at many years in the future before any new standards can be implemented.

So I think it’s -- I think we know enough to proceed with the promulgation of standards that we know are a big improvement over what’s currently in place. I don’t oppose doing a risk assessment but I think we need to recognize the implications and the dangers of waiting too long. It reminds me unfortunately of some attitudes toward the climate change/global warming issue that we don’t know everything so we should study it before we decide what action to take. And I think we know enough in that area to know that action has to be underway even as we study. And I think we're in a similar situation here.

DR. KING:

Okay, thank you. Paul and then Keith.

MR. MILLER:

Thank you. I appreciated Lowell's comments about the subjectivity speculations involved in risk assessment and I, too, looking at, you know, various risk assessments have not been able to figure out how you make some of the evaluations of what probability and plausibility of a particular threat is other than recognizing that some of the speculation that I've seen in public is way out of balance and just isn't plausible. But recognizing that I think is an important element of this and as a result, I think what needs to be evaluated generally speaking when we talk about this risk assessment, it's a risk assessment of electronic equipment and it's risk assessment of electronic equipment in a vacuum. In other words, when you think about all the risks of the electronic equipment without thinking about what the risks are with other alternate methods of voting. In other words there's risks with any system of voting. And so that needs to be evaluated. I think the risks of electronic voting needs to be evaluated in that context because there are -- there is a risk associated with any form of voting.

And the other I would like to suggest that one of the elements of risk assessment needs to look at systems in terms of their ability to detect and correct errors or threats because any risk assessment both is speculation involves subjectivity, but ultimately we can't anticipate every form of risk. So we have to have a form of being able to evaluate these systems in terms of their ability to detect and correct any problems that may occur.

DR. KING:

Okay, thank you. Keith, then Mark, then Alice, then Lowell.

MR. CUNNINGHAM:

That's a good point. I agree. I think that paper is getting a pass in the risk environment or the risk assessment. Everybody seems to associate risk with DRE's. In fact, Russ and I were talking at breakfast this morning, you know if you lose the ballots, where's the paper trail? It's gone. You know if you're transporting them somewhere or what have you.

I think that, you know, the risk thing has just gotten out of hand. I think we've lost all sense of what the opportunity might be. And I think we've lost all sense of what the probability might be, but as a practitioner, I believe the greatest risk to the election system and nationwide is that we continue to legislate it and functionally put it beyond the capacity of the average poll worker to deal with. That's a much greater -- that's a very real risk that's happening on a daily basis is the people that we actually have doing this where the rubber meets the road, do it a couple of times a year, three or four times a year. We all know they're generally older no matter how hard we try to recruit younger people and so forth. And just human failure in the operation of the technology and trying to implement the, you know, the legislative mandates. That's what we're seeing. That's what we're seeing. That's the real risk. That's the real risk that's actually going on as we speak every day. I don't know that we actually have documented evidence of people hacking into machines or doing things like that, but we have human failure evidence in every election.

DR. KING:

All right, thank you, Keith. Mark and then Alice.

MR. SKALL:

Yeah, I want to echo in some degree what Lowell and Paul said. Risk assessment is really incredibly subjective. It's not much different than what we do every single day. We make decisions every day based on either consciously or unconsciously based on some idea of probability we have and the magnitude of the law. So we all make decisions to get on an airplane knowing there's one in a hundred million chance it will crash. Of course the value of the loss is pretty easy to estimate is death. But we make the decision to get on the plane because we don't think the probability is too great and hopefully we're right, but we don't know. We make a decision to drive and the probability there is much greater to have an accident and many of us don't make a decision to do -- I'd love to go hang gliding, I just keep chickening out because I think the probability of screwing up is pretty high, but I may be wrong.

So we make these decisions all the time and they're not always right and they're based on our sort of gut feeling of probability and that's what happens in risk assessment. People make their subjective decisions on probability. Whether they're right or wrong, we will never know. That having been said, I think there's value in doing a risk assessment. The value is not to place all your emphasis on the numbers you come up with because there's going to be subject numbers. The values in going through the process thinking about the risk, getting the community together, and it has to be multidisciplinary. Like you say, the voting officials know a lot about risk. Manufacturers probably know ways to break into their systems. The value is getting the community together, discussing the problems, looking at them, but let's please not place undo emphasis on the numerical results because they are fairly arbitrary.

And I would also echo that hopefully this would not hold up unnecessarily the progress of standards and other things as well.

DR. KING:

Okay, thank you. Alice, and then Lowell, and then Brian, and then Russ. Alice?

MS. MILLER:

I'm just going to basically echo what's been said specifically with Russ and Paul and that is that you have to have a cost assessment. I think is very important. A cost assessment is essential with the risk processes to go through that. And also if you're going to do a risk assessment, you have to assess everything, not just the technology but the paper as well and understand that it's never going to be 100 percent, I believe. Having said that, I think everything needs to be assessed.

DR. KING:

Okay, thank you. Lowell?

MR. FINELY:

I think that paper is getting a bad name in the sense of the often-repeated refrain that paper is getting a pass. And certainly in our state that's not the case. And I actually don't think it's the case with these proposed guidelines. Optical scan systems are also electronic, they use servers to tally and report the results and they are subject to the current standards and to these proposed standards. And in our state, when we conducted our top to bottom review, we had the researchers look just as hard at the optical scan equipment and systems as we did at the DRE systems. And yet there are actually many local elections officials in California who when they get together actually don't know that.

So the other point I want to make about this is that you can't have it both ways in terms of procedures being a guard against possible vulnerabilities or threats. If procedures are going to be sufficient to avoid the potential threats that exist in purely electronic voting, DRE type systems, then I don't understand why they cannot be sufficient to guard against the dangers that exist with optical scan voting. And I think that's something we actually know a lot about and I think local elections officials know a great deal about that. And I think particularly with precinct based optical scan, we actually get an electronic check on ballot box theft or stuffing that occurs right at the time of voting that we didn't have in the past with just traditional pencil and paper balloting. And I think a lot of our stories of times when election fraud did occur, actually go back to those times.

So it's not that it hasn't happened with paper or that it can't happen with paper, but I think we're fooling ourselves if we respond to the concerns about electronic voting by saying that they are at least as great or worse or they're unstudied when it comes to paper ballot.

DR. KING:

Okay, thank you. Brian and then Russ.

MR. HANCOCK:

Thanks, Merle. I think an important consideration that we haven't discussed yet about the risk assessment, you know, aside from the obvious moving forward is that it's going to be a document that needs to be viewed by a broad range of constituents. You know, we need to deal with the cost issues. I think some of the most important people that need to look at that document are federal and state legislators.

There was a great point brought up yesterday at the advocates roundtable that I think needs to be raised here today. And that essentially is that there's a very high level debate that has not really occurred in this country among the federal or state legislators for the most part and that is what level of risk is acceptable? You know, there is sort of an assumption out there that we at this table and frankly the people yesterday and other people agree that, you know, 100 percent is not possible. We know that. I mean that's -- and Mark will tell you not possible in computerized systems, right?

MR. HANCOCK:

But what level is acceptable? And, you know, how much are we willing to pay and who is willing to pay to get to that point? Is it 99 percent? Is it 98 percent? Is it 90 percent? Whatever it is, that debate needs to go to be had at a level much higher than this room right here and it hasn't been done yet. So I think that's one of the reasons we want to put this risk assessment forward.

DR. KING:

Okay, thank you. I've got Russ, and then David, and then George.

MR. RAGSDALE:

Two points and back to my comment about identifying the cost of the mitigation. Recognizing the subjectivity of risk analysis, I would simply suggest a simple possibly three-tiered rating system that the cost is going to be low, medium, or high so I agree.

MR. SKALL:

It's always high.

MR. RAGSDALE:

Absolutely, absolutely, everything's high. It's more an indicator to the election official that they need to explore that particular mitigation. But another element and maybe what I'm suggesting is a risk analysis of the risk mitigation. You need to be careful that the mitigation doesn't have unintended consequences. For example, Deb and I were talking earlier and what seems like what's happening in California is a dampening of the early voting opportunities in Colorado because of the risk presented by the use of electronic voting equipment. That to me is a cost. It is a cost in a reduction of the level of services to our voters. That has be taken into consideration in a risk assessment.

DR. KING:

Okay, thank you. I've got David and then George.

MR. DRURY:

Okay. Well from my perspective it's knowledge based. Number one, the activists, the academics, what is -- sorry about the poor words here. What I'm basically trying to say here is I look at all of this information and have a knowledge base. From that perspective, doing the certification effort, I have to look at the risk. Whether it's there or not and how low risk or how risk, I need to look at it. And if our situation is outside or not inside our bureau, we will have to have an assessment outside of the bureau. Typically, using Florida State University State labs and they would look at this and determine whether there is risk and look at loss, not the probability. And I will look at it from our standpoint can it be fixed with the vendor, if not, what do we do from a mitigating standpoint? And determine that based upon the probability that will occur or could occur. Sorry about all of this. I just wanted to let you know what we're doing here.

DR. KING:

Okay, thank you, David. George and then Paul.

MR. GILBERT:

Well I agree with Lowell that optical scan ballots are not getting a pass from the VVSG. However, manual tabulation of paper is getting a pass. And since we seem to be falling back on the manual tabulation of paper as the ultimate documentation of security of our elections, we are falling back on an unsupported foundation. I think that's probably the greatest weakness that I have seen in the VVSG to date, this new version of it.

In terms of how much risk are we willing to take Brian, I don't think the states are oblivious to that issue and I don't think they have completely ignored it. I agree that they haven't engaged in it. But risk has been around for a long time in elections and all state laws probably accommodate that. In North Carolina, the standard is could the error materially affect the outcome of the election? If it would -- did not, then they will certify the results and declare the winner. If it could have materially affected the outcome of the election, we have procedures in place to respond to that. Sometimes it's called a new election. Obviously sometimes that's not an available option but states do acknowledge this. They have laws in place already that accept the fact that elections are going to be imperfect and the standard generally is do they -- did that imperfection materially affect the outcome of the election?

I think the risk assessment can help us narrow down that margin of error. We are trying to reduce that margin of error. We're not going to eliminate it obviously. So, thank you.

DR. KING:

Okay, thanks. Paul and then Deb.

MR. MILLER:

I'm not sure whether Lowell expects me to agree with him or not but actually I do in this case that I don't think paper has gotten a pass. I also, I agree with him that local election officials are -- have a very good understanding of the risks associated with paper. And I do think that we need to get a better understanding, all of us as election officials, a better understanding of what the risks associated with electronic voting is. And so I am no way opposed to doing a risk analysis but I think it needs to be done in -- and one of our concerns as election officials is the public perception and trust in the systems.

And so my comments earlier were in a sense in that context that if there needs to be in that context an understanding that there are risks associated with all forms of voting. And what we're looking at are the risks associated with electronic voting, but understand that just as procedurally local election officials have developed procedures to deal with the risks associated with paper voting, we are developing procedures to deal with the risk associated with electronic voting and that needs to be part of the understanding going forward here.

DR. KING:

Okay, thank you, Paul. Deb?

MS. SEILER:

I'd just like to comment that I think that a risk assessment isn't a, you know, one time project. That it needs to be an ongoing project and that I think that the EAC could provide a very useful service to everybody including election officials by doing sort of an ongoing assessment of occurrences as they happen whether they're real or perceived problems. And that that could be part of an ongoing risk assessment.

We had a situation recently, I don't know that I agree that paper hasn't been getting a pass but regardless, we had a situation recently in Los Angeles County where and on a paper based system and it went through a top to bottom review where voters had to fill in two bubbles in order to have their vote for a political party counted. It was the double bubble issue, something like 50,000 votes were not counted. This is the risk of voter error. You know, voter misunderstanding the system. And those votes really couldn't be counted. They were ultimately counted but it was kind of high-level guesswork in the way it was done.

So I think that if the EAC could look at these in an ongoing way and maybe come out with some, I hesitate to use the word pronouncement but some assessment of what happened. I mean just to say okay, here is what really did occur and how can we deal with this in moving forward? And that would be an iterative process, an ongoing dynamic process.

DR. KING:

Um-hum, thank you. Keith and then Lowell.

MR. CUNNINGHAM:

I just wanted to touch, you know, I don't think that the technical aspect of paper voting has gotten a pass in these standards. Obviously all of the technical -- the paper itself is what's getting the pass. The security of the paper it's, you know, everything is based on the fact that well, the paper is available. Well the paper, if the paper is not available, if they fall off the back of the truck, if they get lost, if they get wet, if the ink runs, if they smear. If the paper is not available, then I think the whole discussion falls apart. And that's a process issue. Process is what's going to make the paper secure.

DR. KING:

Okay. Keith, I'm sorry, Lowell?

MR. FINELY:

I don't want to get real inside California baseball here but I have to correct the record. That situation in Los Angeles County with the double bubble ballot did not go through top to bottom review at the state level. Our study didn't drill down to the level of particular ballot design issues. And it's also important for people to know that that's a very antiquated voting system that is only used in Los

Angeles County and one other county in the country so it's not optical scan in the sense that most of us are talking about.

DR. KING:

Okay. Any other discussion on the risk assessment? I've heard some really different things here. I think there's a different depth of understanding on election officials. As I was listening, when I was in college, I had the fortune to work for a large retailing company and I can remember having a great manager who explained to me that if I really wanted to mitigate the losses in the store, focus on auditing the invoice and the pricing. And I said, can't I just chase shoplifters like everybody else? And he shook his head and he said, you know, that -- it looks like that, but he said if you really want to improve the bottom line of the store, focus on the pricing. And that was a valuable lesson to me and I haven't thought about it for 30 years until I heard some of the discussion here today about how the election officials really can add value to this risk assessment by understanding at that retail level what the risks are that we face in managing good elections in our jurisdictions.

With that, I think it's time to take a break. The restrooms again are out through that door. You'll need a key, which is on the counter, blue for men, pink for women. And yeah, there's coffee across the street, I guess or around the corner, but let's meet back at fifteen minutes till. Let's take a fifteen-minute break. When we come back, we'll start on Question #3. Matt, if you could go ahead and put that question up and let's take a break.

***

[Recess from 10:25 a.m. until 10:44 a.m.]

***

DR. KING:

I think Brian will join us in just a moment. Welcome back. Thank you for helping us to stay on time. We have four questions that we will cover before lunch. And the third question, which is now being displayed, has to do with at least a perception that election officials value stability as a desired feature of voting systems. That over the life of the voting system there are literally uncounted compensating and mitigating procedures that develop on the fly. Some of them more documented, others are undocumented, but there are ways in which we can ensure that the job gets done with whatever voting system we have. And so often we'll hear that election officials prefer an evolutionary approach to voting systems as opposed to revolutionary. In part because we recognize that there -- it takes time to develop the compensation, compensating features for whatever anomalies are in that voting system.

So what this question drives at is consideration of the unintended consequence of not so much the standard but the voting systems that will be derived from the standard which -- and I think everybody here appreciates that the standard is a means to an end in itself. So in the question could you comment on the value of stability of standards in the jurisdiction that you represent and then which is preferred, a standard with a short shelf life that accommodates innovation and change or a stable standard that may inadvertently or intentionally discourage innovation but creates longer certification lives of voting systems? Some of this I think is impacted by cost which we've heard discussed here today. Some of if is impacted by the things that lead to cost, training of poll workers, familiarity with the system.

So with that introduction, I'd like to open the floor for discussion of this question. David, I think you've got yours up and then George, and then Keith, so David.

MR. DRURY:

Okay. I guess from my perspective that we would like to see short life primarily because the customer wants to have changes. For example, the ballot on demand is one. We've got three different flavors of ballot on demand. We've got Okaloosa distance balloting activity that's going on, the pole being a ballot box. These are all issues here that's causing us problems with standards because there's really none and we're just trying to address it.

DR. KING:

Okay. When you say customers, who are you referring to voters, election officials?

MR. DRURY:

The counties. The counties themselves.

DR. KING:

Okay.

MR. DRURY:

And the voters as well.

DR. KING:

Okay. I think sometimes when we talk about our customers it's a very diverse group, the legislators are included in that perhaps.

MR. DRURY:

Well obviously the distance balloting we would refer to the voter so.

DR. KING:

Okay, thank you. George and then Keith.

MR. GILBERT:

Any set of standards that leaves the impression that there's a perfect voting system will eviscerate itself. There is no perfect voting system and there never will be a perfect voting system. Short life, long life, I'd prefer a set of standards that has no life. And I don't mean by that that it's dead, I mean that it is immortal. Standards need to be -- I mean, we're living in an evolutionary world. We're living in a world where changes are taking place. We're living in elections environments in which different states have different requirements and different needs. The standards have to be flexible enough to meet those needs. If a system is working well in a locality, why are we forcing it to change because we change a standard? The states or the local jurisdictions whichever has that say should be left the flexibility to elect to adopt a particular standard. And every standard that you have is going to employ both technology and management processes.

So if we have a short shelf life, yeah, you need to be flexible. You need to be able to change to meet changing needs, but at the same time, you don't want to force short-term change in the election process. You know both for economic reasons, sensitivity to the voters, the voters like some stability, as well as, election officials. No mater what standard we adopt, it's going to employ certain management processes that fill in the gaps. And for these standards to try to fill all those gaps in a way that leaves the impression that now you've got to upgrade, we don't want to become Microsoft. We're no longer going to support that version, you know. We need to support whatever versions that the jurisdictions out there want to employ with the understanding that yes, we can make changes that improve and improve and when they're ready, they can make those improvements along with us.

So that's my take on it. I don't think we've -- I mean, we need a system that has short shelf life in the sense that it's flexible and long shelf life in the sense that you can stay with something that's working.

DR. KING:

Okay, thank you. Keith and then Paul.

MR. CUNNINGHAM:

The short answer is for heavens sakes, let's find something we can all agree on and lock it down and go with it for a while. The constant state of flux that I think a local official finds him or herself in today is very disconcerting and very difficult to operate in. You know, someone said to me when I first started, you're going to find that every election has its own life. You know and that's true. There are just like little things that occur from election to election well that never happened before and you learn from it. You know, the least we can do is maintain some degree of stability in our technology.

You know, the -- I think the three standards use set forth earlier about, you know, that it's cast right, counted right, collected whatever those...

DR. KING:

Um-hum.

MR. CUNNINGHAM:

...you know, let's not over think this. And I think this document does that with the innovation class. I think that the innovation section of this document allows for and it's a little subjective, but I don't know how else you could approach it, but I think it allows for manufacturers an opportunity to, you know, experiment. And we sort of don't want to kill that but, you know, let's again, let's not over complicate or over think of this. In most cases, you've got a yes or a no or Candidate A or Candidate B and, you know, we can come up with all sorts of elaborate ways to collect and count those but -- and I'm sure in the future there's things we haven't even thought of.

I think one of the problems we're experiencing though is just the exponential increase of technology. Most boards that move from punch cards into DRE's without any sort of thing in the middle so, you know, that -- but when you've got to retrain, you know, getting back to the let's stabilize this as much as possible because every time you've got to retrain yourself, your staff, your poll workers, your voters, your media, your advocates. I mean, every time you've got to retrain all those people it's just time you're not spending actually running an election and making sure you've got everything going right there so.

DR. KING:

Okay, thank you. Paul and then Lowell.

MR. MILLER:

As a state official, I would certainly agree with George and Keith in terms of the importance of having stable standards. And, you know, our attitude in Washington is that if a system is working well for a county and they've learned how to compensate for it or even if it's loss or weakness, they're certainly more reason to decertify the system and force them onto a newer system except where HAVA or federal law requires them to do so.

However, I do think and Keith made this comment about the exponential technology. As we're well aware of New York probably has had their election machines for 100 years now. We had punch cards in Washington for I think 30, 40 years. And that is sort of the expectation in the elections community that that's the life cycle of the elections technology. And that's also sort of the funding cycle for elections technology, unless it breaks, unless you have a spectacular failure.

But I think we need to recognize in terms of the stability of our standards is that the exponential technology is overtaking us. In our offices, we think nothing of trading out our PC's every three years. If you have Windows 95 in your office today that's only, you know, that's less than ten years ago but five years ago it was obsolete. And I think we're going to see, I expect to see some of the same kind of things in the elections industry as well because of the use of computers. Those are basically off the shelf type of equipment and people going to the polls and voting on a 286 is not going to be struck as that's a reasonable technology to be working with.

So I do think that there's going to have to be a more frequent cycle than we've had in the past. What that cycle should be is not clear to me at this time, but my expectation because of the technology is that it's going to have to be shorter than it has been in the past.

DR. KING:

Thank you. Before we go to Lowell, whoever has the WiFi device that's close to the speaker, if they could silence it or move it back away from it that would be a great thing. There's a Bluetooth or a WiFi humming in on something. Okay, Lowell?

MR. FINELY:

Well I want to take the opportunity to respond to a couple of points that have been made in the discussion so far. One is that, you know, there's the old saying don't make the perfect the enemy of the good. I agree that we can never have a perfect voting system, but I don't think that that's a reason not to attempt to develop standards because I think that standards can help us go from where we are now which I think is poor to good. And because we can't get to perfect in part and because of all the needs for, the need and benefits of stability from the point of view of cost, from the point of view of the comfort of poll workers and the training required, the understanding of the voting system by voters, I think that a set of standards that is long lasting on balance is preferable. I say that with the caveat that I think it's only viable if open ended vulnerability testing and software independence are part of those standards because what we don't know now and which is inevitably going to be developed are new ways of attacking any kind of computerized system, any sort of software in a device. The people who do that never rest and they're always coming out with new things. And the only way you can have any chance of keeping up with that is by not only studying what is being done on the dark side, but also doing open ended testing that's not tied to a standard that could be shaped right now and unable to anticipate the future.

In terms of concerns about obsolescence and, you know, new standards forcing people to give up old systems that have been working for them, actually I think that's not -- none of the standards have been retroactive. They've all been things that apply to newly certified and newly purchased systems. And I think that's really an issue more of the sophistication of contracting practices by counties and in those states where it's done centrally by the states in dealing with the vendors and looking to the long-term future when they consider the contracts that they enter into. You can't have support for your system pulled out from under you if you've written protections against that into your contract with the vendor. And I think this is somewhere, a place where interaction amongst elections officials around the country can be very beneficial.

And I guess the final point I would make is that we need strong standards that are widely adopted around the country to benefit each state because each state is vulnerable to things that might go wrong in other states and it reminds me of the saying that people tend to love their own representative in congress but hate congress and fear it. And I think we tend in each of our states and each our counties to believe that we've got good procedures and systems, we know how to do it, we don't need to be told what to do. But each of us is vulnerable to any state or any county that doesn't do a good job. And when it comes to security of voting systems, if they're stolen, if there's an intrusion anywhere in the country with a particular voting system that threatens the security of everyone else in the country. So I think that's something we need to bear in mind.

DR. KING:

Okay. Now looking at Alice, you had...

MS. MILLER:

Yeah, just briefly.

DR. KING:

Um-hum.

MS. MILLER:

I think that you need to make certain that there's room for change with the equipment and with the process and all of that, but I also think that stability is very important. So it's a balance between the two. I know, you know, from the perspective of having to recruit and train poll workers, they do not accept the change or institute it easily and it's a very challenging kind of process. Also the voters don't always understand, you know, why we're changing from this to that. I -- just personally, I know when we started the dual system with the DRE and the optical scan, we had initially the year before we institute the DRE, we had put the optical scan in place and they were very comfortable, had developed a comfort level with that and then we got the DRE and the optical scan four years ago. As of my election in February, I still have poll workers that will not set up the touch screen machine. They just won't do it. So, you know, we're out there trying to tell them you have to do this, you know, it's a requirement for accessibility issues, we're adjusting the training materials and the manuals so that they understand how to process everything on the dual system.

So the change part of it is while it’s important, stability I think is just as important for those reasons for the voters, the poll workers, the training, all of it. You know, there has to be a balance, I think, but stability is important.

DR. KING:

Okay. Deb?

MS. SEILER:

I’ll just echo what Alice said. I think -- and I think that maybe true the larger you get, I’m not sure if it’s size related but I think there’s a maturation process in all of this with your voting system. I -- what we’ve seen with some of the sort of Legacy systems is that these systems have been in place for decade and they’ve been allowed to sort of mature both with respect to the management processes that surround them, as well as, any technological tweaks if you will that have been allowed to occur. And I think we need to take the same long-term approach to this.

I mean, Alice is absolutely correct. Every time there’s a change -- we’ve not had the luxury in San Diego of running an election, a major election the same way twice since 2003. And the toll on that in terms of our poll workers, our voters, our costs, our costs have tripled, just our operational costs. Every election we have to rework our whole manual. We have to restructure our warehouse. We have to try to reeducate the voters. It’s just been really very difficult.

So I can’t emphasize enough how much we appreciate stability, but having said that, the standards need to help us somehow keep moving through the process where as we identify things that can be improved and maybe it's security, maybe it's a process that we have the flexibility of doing it.

DR. KING:

Okay, thank you, Deb. Russ?

MR. RAGSDALE:

I think it was in the October training session with NIST, I believe Professor Skall was lecturing us on a good standard address performance not design. And I think if the standards, in fact, address performance like Keith pointed out, Merle that you stated the three tenants of best performance, it's not design. This is what it should do it's not how it has to do it, that you create a set of standards that are durable and stable and allow innovation within those standards.

DR. KING:

Okay. One other reflective question back out to the panel. The -- I often think about the six blind men and the elephant parable that works in elections in so many different ways. Whatever part of the elephant you stumble across, it seems to define the unseen animal. And the standard is and of itself certainly the focus of this discussion but it's only a piece and so when we change a standard, we then have to look at unfreezing perhaps what we've been doing, assessing and refreezing. When we change the standard and then we change the metrics by which we measure conformance to the standard. When we change the metrics, we change the protocol of the testing lab. When we change the protocols in the testing labs, we change the behavior of the manufacturers to come into compliance. So it sets in motion a chain of events that we've had a couple of iterations of this and I certainly don't pretend to have a handle on what the lifecycle is of implementation of a standard but it's certainly longer than I think many of us would like.

And so going back to kind of the tip of the iceberg question that the standard is and of itself only a small revelation of a mountain of hidden actual cost and opportunity cost underneath it, I'd like to come back to really the first two comments here that I heard David say which is we need adaptability within the standard. We have demands coming in from customers. We want to stay active in the federal certification process, but then I also heard from George flexibility with stability, finding the most, the best of those.

And I think also Deb, your observation that larger jurisdictions it looks a little different to us and I'll speak briefly about the jurisdiction I represent. When we decide to make a technology change, the threshold is so high now it could well be $100 million for us to make a change in a system because we have the uniform system. So I think the problem does also look different depending upon the size of the jurisdiction involved.

But I'd like to kind of throw it back out for a reflection on this question about the life of the standard in the context of all of the cost that sit behind the curtain of that standard that have to be dealt with both in terms of time and actuality. Lowell?

MR. FINELY:

Well, I think we've seen a dramatic example of just a simple, a single standard resulting in extremely large unexpected or unanticipated costs and this was the provision in HAVA not in the voting system guidelines, but the provision in HAVA that was especially early on widely interpreted as mandating the use, the acquisition and use of DRE's. And one of the hidden costs of that which we've seen, you know, being discovered in a kind of serial fashion state by state, county by county, and especially county governing boards are shocked when they learn of this, is the cost of storing DRE equipment, computerized equipment like that where you have a large number of DRE units that are required for each polling place if you're going all DRE. And they have to be stored in not only very secure but also in air conditioned facilities. And this has come as a, you know, a real shock to a lot of local jurisdictions.

So I agree that there are hidden costs and that everything that can be done to anticipate those, to sort of stand back and try to identify those in advance that that's important both in deciding whether the standard is affordable, but also from the standpoint of approaching the contract negotiations in a wise fashion. Debra Seiler's county, San Diego was very farsighted in writing a contract with its vendor several years ago that required the vendor to provide a replacement system if for any reason the system that they had purchased was not in a certified state. And others have put in provisions that required the vendor to provide a voter verifiable paper trail system at no additional cost if it came to be mandated by law. So it's not just a matter of identifying the cost, it's also a matter of identifying how that cost is going to be born and distributed.

And I -- and last point, I think it's very important that those costs be internalized. And if it means that the cost of initial purchase of the voting system and the maintenance contracts goes up, I think that’s actually better so that those who are making the decisions about costs and preparing different systems that they might acquire recognize what the true cost is in trying to internalize all the costs and put it into a single price tag instead of have it hit in a series of unexpected additional hits later.

DR. KING:

Okay, thank you. I have one other question of the panel and then I think we do need to move onto the next. Paul had mentioned and I don’t know seriously or tongue in cheek but perhaps 30 years is the amortization schedule for voting technology or maybe 100 years if you’re in New York. I’m curious in the jurisdictions that you represent; do you get a sense of what your funding sources view as a reasonable lifespan of a voting technology? I’ll start with George and then Keith.

MR. GILBERT:

I think their expectations of changing with the changing reality as well. I’ve used DRE systems for 20 years. I’m in my fourth generation of the DRE equipment. Of course that wasn’t anticipated 20 years ago. But with the, you know, with whatever -- we’re using electronic technology in elections period. And counties are -- awaiting that electronic technology doesn’t have a 30-year lifespan. So I think that expectation is changing along with the rest of the market and the rest of the environment that we all live in so.

DR. KING:

Okay, thank you. Keith and then Deb.

MR. CUNNINGHAM:

Well I think your funding authorities like county commissioners probably feel it should be 50 to 100 years because heck you only use it a few times a year, I mean -- but I think that at least I believe right now that probably ten to twelve years is about the lifespan of any system. And when I speak with my commissioners about it that that's -- we had an optical scan system in -- that we put in in 1995 and we put this new system in in 2005 so -- and that old system was beginning to show wear and beginning to technically be outdated so I think again back to the just exponential increases of technology, we can't expect anything to probably last more than about ten years at this point.

DR. KING:

Okay.

MR. CUNNINGHAM:

But the other, when you said the other cost, you know, there's also in addition to the technical costs; I mean just the physical costs. Because if a, you know, I know many people whose boards of elections went from punch cards right to DRE's and, you know, in a punch card operation their little punching devices stayed out at the polls all year and they just, you know, took ballots out. Now they've got rooms and rooms of equipment and they need to deal with delivery and all kinds of issues that they never had before. It's causing a lot of problems.

DR. KING:

Okay. Deb?

MS. SEILER:

Yeah, I don't know that there's a good answer to that. I think there's so much uncertainty anymore that, I mean, and I agree with everyone else who said it used to be, you know, 50 years was, you know, you'd think 40 to 50 years...

DR. KING:

Um-hum.

MS. SEILER:

...was the lifespan of a voting system. But now I think that, you know, election administrators see that or county supervisors see that there's a cost beyond just the monetary cost. They are sort of waking up to the fact that there's a definite monetary cost and they're starting to think about how to budget for that, how to plan for that, maybe we built it into building per jurisdictions or something. But there's such a political cost to it, too. And we don't know even if we go out and make the expenditure would we even be allowed to continue that system.

DR. KING:

Um-hum.

MS. SEILER:

So I think there's a definite pulling back. You know, if we could, we're going to spend $25 million on one system and then not be allowed to use it are we going to pull back and just say no, we're stopping, we're just going to become very conservative.

DR. KING:

Okay, thank you. Paul?

MR. MILLER:

I do think that there may be a -- needs to be a differentiation between large counties and smaller counties. I do think the expectation of the smaller counties is still that there's this longer lifecycle to it. I think the larger counties are recognizing, beginning to recognize that it's shorter than what they used to expect.

DR. KING:

Um-hum. Okay, thank you. George?

MR. GILBERT:

Frequently in recent years used the term statutory obsolescence to apply to...

DR. KING:

Um-hum.

MR. GILBERT:

...the voting systems so that is what we've experienced. We haven't experienced the obsolescence of the equipment. In a technical sense, we've experienced statutory obsolescence.

DR. KING:

Um-hum.

MR. GILBERT:

We may experience VVSG obsolescence. You know, those are the things that I think are driving the train at this point. Local jurisdictions don't have any option but to respond to statutory obsolescence. They don't get to consider the wisdom or the merits. And the same thing can happen with the VVSG. And I'm hoping that the VVSG standards will be written in a way that they do not appear to be statute. That is what I was trying to refer to in my original statement about the perfect voting system. Obviously no such thing exists and we don't want the VVSG's to create the impression that, okay, there's a better way to do it you've got change. So that's what I'm hoping we can do.

DR. KING:

Okay, thank you. Russ, I thought you'd say day to day (inaudible). Matt, could we move on to Question #4, thank you. Question #4 is dealing with open-ended vulnerability testing and Lowell's volunteered to make some introductory comments on that.

MR. FINELY:

Okay. I figured that we were going to be getting sleepy at this point so maybe this will be provocative. I hope it will generate some discussion. Open-ended vulnerability testing we know has been referred to as OEVT. And we have such a proliferation of acronyms in this whole business that I thought I should add a couple also, yeah. So but I'll explain them. That's what PowerPoint's are for. The first is MVA and the first is IIDAT or IIDAT for short.

The next slide, please. Now MVA stands for misnomer based antipathy. And I think that this is what we're facing when we talk about open ended vulnerability testing because, in fact, it's not truly open ended if you look at the VVSG or if you look at jurisdictions that have attempted it on their own. It's not really a matter of wide-open techniques. The techniques that are used in penetration testing and source code analysis are widely known. Probably what matters most is the quality of the people, experience and training of the people doing the testing and the mindset that they bring to the job. Do they think like cat burglars and criminals or do they think like regulators? And if they think like regulators, they're not going to do a very good job. But it's not wide open.

The cost is also not unrestricted. We went through a process in California that we estimate on a long-term basis is something that could add in the neighborhood of $250,000 to $400,000 to the cost of testing a system. I don't think a monetary value has been placed on what's proposed in the VVSG but I don't think it's outside that ballpark. And the time is not unrestricted. Even if this weren't written into the guidelines, there's a lot of practical pressure to complete the job of testing systems. And I think that this was certainly the case when we did our top to bottom review. It was the case with Ohio. Even in a short time, you can learn a great deal of valuable information so, next one.

Now IIDAT is my proposed alterative to OEVT and that is insider intelligent design attack testing. And I'm particularly proud of getting intelligent design in there. Insiders as we know from a lot of industries and fields of endeavor are usually the greatest threat to any system whether it's computerized or otherwise. Insiders know the system and insiders are in many ways the hardest to monitor whether they're vendor insiders or they're IT insiders in the governmental structure or consultants. So I think the focus needs to be shifted heavily in the direction of testing for the dangers of insider attacks. I think we have to recognize that those attacks are likely to be very intelligently designed by people who know what they're doing. That the resources are there to hire those people or the motivation is there for the people who are doing it for free given what's at stake.

Next slide.   So why should we use whatever we call this with voting systems? And I think the most simple answer is that it works. Open ended vulnerability testing or IIDAT finds serious vulnerabilities have been missed by other testing and I just think there's nothing more dramatic than the fact that we have a whole series of federally certified voting systems in the field that have been shown in several rounds of open ended testing to have wide open security vulnerabilities. And I can tell you when we speak to them in private the vendors acknowledge to us that those vulnerabilities are there regardless of the statements they make when they come before us at public meetings. They don't have an answer to the vulnerabilities that have been identified.

And I think this kind of testing is important because it answers the right question. It doesn't tell us whether a system meets a particular set of criteria. What it tells us is this system vulnerable to attack? And that's what we really need to know given what it is we're trying to protect from attack.

I think there are good and bad reasons to be testing for security. The good reason is to identify real attacks, attack vulnerabilities and fixes and defenses. The bad reason to do it is to guarantee that vendors will have their systems certified if they meet a security specification whatever it is.

Obviously there are views very unlike mine on this topic. And I'll just address a couple of them. One proposal has been to use this testing or to reorient it so that what we're testing for is not particular attacks or vulnerabilities but rather testing for the quality of the software development process that was used to create the system or process maturity. Another alternative view is that testing should be done in the real world or it doesn't really have any meaning in the real world. And the final and very popular alternative view is let's just skip it.

So let's go to the next one. The development process maturity alternative is one that was proposed in the first of these roundtables by Professor Yasinsac from Florida who has been involved in open-ended vulnerability testing. And his proposal is to test for again how mature is the development process used by the vendor who developed the software. The rational for this is that if you follow good development practices, you're likely to avoid common security vulnerabilities such as buffer overruns and there are a number of others. His second major argument is that open-ended testing is inevitably going to have diminishing returns. Eventually we won't find any attacks in the systems and so we should be looking to the longer term.

Next one. The problems I see with this is first of all which standard do we adopt and what kind of meaning is it going to have? In his paper, Professor Yasinsac proposed use of something called CMMI, which is an industry standard capability maturity model integration that's been around for 30 or 40 years. I understand through various iterations. There are five levels to which a system can aspire. Level 1 is initial and I love these characterizations that are given for it. It's chaotic, adhoc [ph] or heroic level of programming. Two is repeatably. Three is a defined institutionalized development process. Level 4 is where that process is highly managed in a centralized way by the enterprise.

And Level 5 is a system in which the process is constantly being optimized and developed.

The problem is what do we do with a standard like that? Most sort of major off the shelf systems that we rely on all the time are at Level 1, Apple, Microsoft, Semantic Security Software, and I found this example interesting, the Brazilian Electoral System Court is qualified at Level 2. Most mission critical systems are in the three to five range. And particularly defense systems are in the four and five category.

So where would we place voting? And if we did adopt such a system would it give us a false sense of security, which in my view is worse than having no security at all. And I'll just give the example of bicycle locks. When it became clear that people could bring a big bolt cutter and cut through cable on a bicycle, the new gold standard became these U locks that are made out of hardened steel and locked with a key lock. All the focus was on the hardened steel and everybody went out and bought these until someone discovered that you could break the end off a Bic pen and use the hollow barrel stick it into the lock and pop these things open. So if you think you've got a good security system in place and it isn't, you've got a worse problem than if you didn't think you had any security at all because in that case you probably wouldn't leave the bicycle outside, you would bring it inside with you.

The argument for testing systems in the real world obviously this is appealing and had a lot of common sense appeal to it. In the real world of elections, security procedures prevent or reveal the existence of tampering. And, in any event, the only ways in which systems have been cracked is by the world's top computer security experts being given access to everything in a laboratory and relatively unlimited time. Again, here are the problems. It's impossible to test the vendors operation in a real world scenario. No vendor is going to let regulators come in and supervise and observe their entire process. It's literally legally impossible to test procedural safeguards in a real election scenario. We simply can't be attempting to hack into systems while an election is underway as a means of testing them.

The real world alternative and its reliance on procedures makes a very big assumption also which is that thousands of people who are involved will strictly comply with the procedures and, therefore, we shouldn't worry that much about the technical vulnerabilities of the systems. Also, we know that several viable attacks don't require the attackers to be experts and yet conversely the biggest threats do come from experts and those are the ones that are going to be hardest to detect and to manage through procedural approaches.

And this is let's skip it. If it ain't broke or literally if it ain't been broken into, then we shouldn't test it. The argument is frequently made that we've had hundreds or thousands of perfect elections with electronic voting systems and certainly not proven case of fraud committed on them. That the fraud that has been proven has been on paper ballot systems and that doing this kind of testing given that setting just undermines voter confidence in elections.

The simple response I have is we don't know if E- voting fraud has happened. What we do know from our studies is that attackers can completely cover their tracks in the current systems because they can go in and change the audit trail so that they match up with the changes that they've made in the system. And we also know that auditing of elections whether they're on paper or electronic systems has historically been weak to non-existent in terms of probing for security breaches. And my contention is that if E-voting fraud is possible and I believe we know that it is, then it will happen if it hasn't happened again because of what's at stake.

And the little story I just want to tell here, a corny joke that my father always used to tell was that back in the 60's a beatnik was standing on the corner of Hollywood and Vine and snapping his fingers and someone stops and says, now why do you always stand here snapping your fingers? He says well it's to keep the elephants away. The person says but there aren't any elephants around here. If we're convinced that something simple is keeping us safe from a serious problem and we don't know whether that problem is really present or not, I think we're in trouble, so knowing is better than not knowing.

And here is where I resort to what is known in the computer world as the brute force attack which is essentially if the EAC does not adopt open ended vulnerability testing or IIDAT, I can assure you that California will. It will be costly. It will add months to the end of the process. We know that that's what we do now. And we'll continue to do it until a robust set of standards and testing is in place on the federal level. We have one in ten of the nation's voter's. We have market power with the vendors and we're not the only state that feels this way. So with that, I'll throw it open.

DR. KING:

Okay, thank you, Lowell. Any follow on discussion?

MR. CUNNINGHAM:

I don't know how I'm going to get up and go to work Monday.

DR. KING:

Okay. George, then Keith.

MR. GILBERT:

Well Lowell's expressed one view and I think Alice had expressed one view and without even attempting to address all of the different views that other people hold on that, I guess my reading of what is proposed in the standards and some of the alternative interpretations of OEVT, do threaten to overburden the process both in terms of time and cost and I think that that clearly needs to be avoided. OEVT could also be interpreted in a way that eliminates the needed flexibility in system development and standard development, particularly in system development. And we've already discussed that and I think addressed that need as one of the needs in the process. Being able to respond to needed changes in software, hardware, whatever in a timely fashion without incurring, you know, huge costs.

And beyond that, I would simply say that whatever views are in opposition to those expressed by Lowell, I pretty much agree with them.

DR. KING:

All right, George, thank you. Keith?

MR. GILBERT:

Especially the expert opinions...

DR. KING:

Keith and then Paul.

MR. CUNNINGHAM:

Yeah, I think open-ended vulnerability testing has a place obviously and I agree. I think you need to know, but I think it's important that we not let it become the hypochondria of what we do because it is, in its purest state is simply open ended vulnerability testing, there -- it has no limits. It just continues to feed on itself. It -- as I believe we understood from the NIST folks in Colorado it can never tell you if a system is secure. It can only determine it. So I think it runs the risk of having the same effects as hypochondria does on individuals.

The -- I want to take exception with the line about assuring the compliance of thousands of people. You know this is a human system. You know, I have on Election Day 50 optical scanners deployed but I have 600 people deployed. And, you know, if I cannot rely on those people that I've worked with and hired and the staff in my office, then I -- there's no reason for me to go into work on Monday. There really isn't. And I just, you know, I don't know maybe in California, you know, we have good water in Ohio and it keeps us, I think, a little caught on balance, we're not quite as -- not that it can't happen but I tend not to want to be too hypochondriac about this.

DR. KING:

Okay, thank you, Keith. Russ and then Paul.

MR. RAGSDALE:

I agree with Keith I think in whole, I think OEVT has merit, absolutely. It's an industry standard in a lot of technological industries and but my question is and maybe I'd pose this to Brian or Mark. How is OEVT being deployed or employed in other technologies, in other fields, other industries that require certification? Is it part of within the parameters of a certification program or is it outside and used in the -- in solely the product development arena?

DR. KING:

Okay. I know Mark's got his flag up but let me go to Paul first and then we'll come back to Mark.

MR. MILLER:

Well I was wondering if you -- Merle if you were going to address the rest of this question because I'm interested in the answer as well.

DR. KING:

Okay. Let me defer that to Mark and then we'll come back to Paul. Yeah, Paul, make sure you speak into the cordless mike.

MR. MILLER:

Okay.

DR. KING:

Thank you.

MR. SKALL:

Yeah, I think I'll get to Russ's questions somewhere in my response. A couple of issues. The cost, OEVT costs money like everything else. The bang for the buck is pretty good I feel. If you look at what the total cost is going to be to deploy a system and test a system and you look at the cost of OEVT, it really is a fraction. So I think the cost thing is just a little bit -- if you want to worry about cost, throw away the whole standard because that's where the cost is. I mean we have a lot of good requirements and you have to pay someone to develop a system that meets these requirements and test it. The numbers for that are fairly high and there's no doubt about it, you have to pay for that. OEVT really if you stick to like twelve weeks is what it says in there of staff time and that's not really all that substantial.

It is standard practice typically in development of systems. It's typically done. I think Russ's question was about is it within the standard? That's where the tricky one comes. I know of no other standard that actually mandates this. Usually it's done outside of a standard environment. And there are some problems. I have to admit of putting it in the standard because it is not the objective measures that we would typically like to see where you'll be able to make a real easy determination of compliance or conformance.

And the second one that no one's brought that has always bothered me, of course, I think we need to find ways around this is the consistency across labs. Since there is a degree of subjectivity, how do we assure that there's no forum shopping. How do we assure that you get the same results when you go to Lab A versus Lab B? I've had some thoughts perhaps of assigning a team. Rather than having a team from each lab, maybe have a team across labs or representatives of labs to ensure that this sort of one team that we always have the same results.

But there are options. You could take it out of the standard and make it part of the certification procedures. We've talked a little bit about that. I don't know where it should be. This was the best attempt I think of the TGDC to ensure it happens. If there's some way you could do it outside the standard and we can ensure it happens, I would be in favor of that. But I think it's an important thing. I think you learn a lot and you just find things that you wouldn't find if you don't do it and that's the business we're all in to try to find problems.

DR. KING:

Okay. I'm going to also let Brian weigh in on this answer.

MR. HANCOCK:

Yeah, I just want to kind of back up what Mark was saying. We -- it's certainly something we've talked about and discussed and I think actually the TGDC probably had some discussions, at least the sub groups had some discussions about this. I, too, think it's a very important aspect of the whole process. I am not sure if it belongs in a certification process. Like Mark, I think in most industries and I'm not the expert that Mark is in other industries but I believe it's generally done more in the development process than in the certification process. But I do agree that it's an important portion. It's an important part of assuring the systems are secure.

DR. KING:

Okay. I've got Paul, and then Lowell, and then George you get the last word on this question. Paul?

MR. MILLER:

Well I also agree that it’s an important part of the process and I would -- as far as my perspective from the TGDC, I would much prefer to see it being done in one place rather than five different states doing it. I have concerns about how it is implemented and concerns again going back to that issue of dealing with our responsibilities of election officials to portray an accurate picture of what the risks are associated with using these voting systems. And the -- and so I believe the way that this kind of testing is done is perhaps part of the development cycle but my understanding is that it’s also done as part of the implementation. That it’s often done in the industry as part of the implementation process for companies to understand what their risks are using that system and to develop procedures enough that it’s for mitigating that. And I think that if there were a process that we could -- a way that we could use this OEVT to help election officials understand what the risks are and what we need to do to mitigate those risks, I think that would be a helpful part of this process.

DR. KING:

Okay, thank you. Lowell and then George.

MR. FINELY:

I just want to reinforce Paul’s point. Penetration testing is done widely after systems are installed both in private industry and in government. And it’s done sometimes with the knowledge of in house staff and sometimes without their knowledge and only the top people in the company know that it’s happening. And it’s a critical tool in identifying vulnerabilities and mitigations. Our IT Department at the Secretary of State’s Office does it.

DR. KING:

Okay, thank you. And George.

MR. GILBERT:

I didn't want to leave the impression that I'm opposed to OEVT because I think what I'm concerned about is how it's done and that issue has been addressed by several of you. Both Russ and I, I think addressed in our written remarks that if it isn't implemented as a pass/fail type of process, it would likely stop the whole process. It is said that every system has its vulnerabilities and there's somebody out there that can find them. And that's probably true. So if you implement it as a pass/fail standard in the standards, then you're automatically cutting off the process and nothing's going to pass except by chance.

But using it in conjunction with system development, I think is an excellent idea. Lowell mentioned that the vendors aren't going to invite us in to, you know, well they don't have to invite us in. We can tell them we're coming in. We tell the vendors they have to do a lot of things they don't want to do. So, you know, if it's a part of that development, part of that evaluation process, it has a very different context than if it's a "standard" that they can pass or fail. When you identify a vulnerability, what is the public reaction going to be? Oh, that system has a vulnerability, throw it out. That leaves us with nothing. That leaves us with no systems. So we don't want to create an environment in which that occurs. I think Mark acknowledged that it has to be used very carefully but it certainly can be a very effective tool in us identifying vulnerabilities and planning means by which those vulnerabilities can be addressed by the voting community, by the administrative community itself so.

DR. KING:

Okay. And Deb, if your comment is real brief.

MS. SEILER:

Oh, just -- okay, very brief, because I agree with a lot of what George is saying here but I guess my concern is the negative image that it seems to have, you know. The sort of inherent accusation that we as election officials are stealing our own elections, our rigging our own elections, and then also the concern about, you know what standard is there for paper? Because I think everything has been pointing to accounting systems and, you know, if you're going to give a whole stack of paper ballots to somebody for twelve weeks, you know, what could they do with them. So again, you know, so that there is some context for this testing and some way of trying to mitigate the, just the terrible negativity for election officials.

DR. KING:

Okay, thank you. Well keeping on track if we could move to Question #5, Matt? One of the issues that's been expressed in several of these roundtables has to do with the distinction between system testing versus component testing. And right now there are concerns that have been expressed by particularly the vendor, the manufacturing community that if every small change to a system requires system certification, the cost and the -- in both effort, time, as well as, money will increase and possibly depress innovation or depress required changes in voting systems. So the question here is would component testing which is the ability to test and certify components as they're modified or added be beneficial to jurisdictions? I'm seeing headshaking and Deb?

MS. SEILER:

Well I -- to me I think the question is yes, absolutely yes. Obviously and I was talking about this earlier, the need for some maturation. I don't know -- as much as we would like to have the perfect standard and the perfect voting system, until it goes through all of its iterations across maybe even a four year election cycle, I don't know that a system is truly tested. And, you know, can we think of everything? Can we catch everything? I don't know. I don't know whether that's realistic. And there's also the issue of new improvements in technology that come down and could we just take advantage of those without throwing out the entire system which is such a totally painful and expensive process. So for us, I mean if we could somehow retrofit our system to make it viable, wouldn't that be a good thing? I think we would all be winners if it could.

DR. KING:

Okay, thank you. I've got Russ, and then Brian, then Keith, then George, then Lowell, then Paul.

MR. RAGSDALE:

I'll keep mine brief. I would not be a proponent for component testing. If the EAC could figure out a way to suspended all state legislators from affecting election legislation...

DR. KING:

I admire your brevity, Russ. That's well said. Brian?

MR. HANCOCK:

Yeah, I don't think so. Frankly, you know, just given the development of our certification program over the last year, I have certainly become a believer that component testing is where we need to go in the future. Just there are some significant barriers right now to component testing. You know, certainly the process of modifying and certifying current systems takes money, you know, it's going to cost for everyone. But certainly, component testing would be a see change and certainly a large cost first off on the manufacturers. Right now, we don't have any common interfaces for different components of voting systems that can be used across platforms. You know, so those would need to be developed, you know, as Mark knows and NIST actually discussed. There are certain languages that are available but haven't been implemented into voting systems yet that would let those components talk to each other. So I do think in the future that is where we need to go to make the program more flexible for election officials and perhaps more cost effective but it's going to take a while. And it is believe me going to be a see change for the manufacturers.

DR. KING:

Okay, Keith?

MR. CUNNINGHAM:

Well just quickly, yes, and I think it's the key to perhaps doing what we talked about earlier, developing a standard that is stable but allows for some flexibility to occur as we progress through technology changes.

DR. KING:

Thank you. I've got George, and then Lowell, and then Paul.

MR. GILBERT:

I thought I knew what we were talking about until I heard Brian just a moment ago, which confused me substantially so I won't ask him to restate that, but at some point you can explain to me what you said. Apparently component testing has -- makes different impressions upon different people with what it means. My observation has been that we have applied the testing standards or the certification standards to some things in our industry, which are superficial. And I think the standards need to somehow address that. If you move a chip from here to there in the machine, you decertify the system because you didn't get permission to move that chip. That I think is missing from the standards at this point and it needs to be addressed. Whether that's in the context of component testing I'm not sure anymore.

But that's a -- and the other thing I had experienced is when we have found flaws in the system which we have on a number of occasions over the years; we used to be able to fix them quickly before the next election. That's no longer possible. There are known flaws in the systems that we have that cannot be fixed because it's taken a year or two to get certification of the new updates. And I've got to continue to run elections with known flaws in my software. That's a problem.

DR. KING:

Okay, thank you. Lowell, Paul, and then I'm going to let Mark have the last word on this topic.

MR. FINELY:

I actually just had a question for Mark. Can you discuss to what extent interim testing a system that's been through certification but where there's been a modification to one or two components is that something that could be done in a shorter time and at less cost under the current proposal?

DR. KING:

Go ahead, Mark.

MR. SKALL:

I was going to wait until they go and I'll address that.

DR. KING:

Okay, then Paul.

MR. MILLER:

Well my comment was going to be similar to Lowell's which is in my understanding of component testing means that the system is -- has been certified as a whole and they come back and they've made a change to the DRE or something like that where you're testing the DRE and not the entire system. And then so I had a question about what place regression testing. And so if you're raising the flag and shaking your head suggests that I'm not understanding correctly what you're proposing.

MR. HANCOCK:

Well I think what you're really talking about is testing modifications, which is really what George was talking about. And, you know, I'm not so much sure that what it -- what George was looking at is part of the standards but probably should be part of the certification program. When I was talking about component testing, I'm talking about being able to use pieces from different manufacturers. You know, people that might not even exist yet. And just a real simple example is for accessibility purposes, you know, there might be someone out there that has a great component that they would like to sell, you now, but that's all they do. They're really good at accessibility, that's all they do, but currently, you know, there's no interface to have that product off to voting systems and there's no way that we would certify that product outside, you know, the process of certifying everything. You know so that's more what I was talking about.

MR. MILLER:

Something like an Automark?

MR. HANCOCK:

Yes, sort of, yes.

DR. KING:

Okay. Mark?

MR. SKALL:

Yes, so just back to Lowell's question. I think Brian answered that. I hope he did. That that issue really is outside of the scope of the standard. That's an issue to be made by the certifier, which in this case is the EAC. But I want to ask a more fundamental question. A system is more than the sum of its parts. The whole is more than the sum of its parts. So what are we actually gaining? You know I've always had some issues with this as a tester. Typically you test and make sure that in fact the system works. And, in fact, when there's any change as we all know to a piece of software or even hardware that it integrates with the system we have, unless you can really isolate it and I know you try to do that in the certification process. Unless you can really isolate it, how do you know the system works? So we have a bunch of certified components and we put them together, that doesn't mean that the system will work as intended. So I guess my question is what have we really gained? What are we going to do with these parts because when we put them together, we have absolutely no assurance that the system itself works and that still has to be tested? So that's just a question I'm throwing out.

MR. HANCOCK:

Well I'll just try to answer that very quickly and then we can be done with this. You know, I agree. I mean the system would still need to be tested as a whole. We need to make sure it works, okay. I think what we're gaining is entry into the market of innovative products that currently wouldn't be able to get into the market in any other way. You know, when the Automark folks were first trying to sell that thing, they wanted to sell it as a component. They couldn't do that under the process that existed then or certainly exists now. You know, I think there are a lot of good ideas out there from manufacturers that don't necessarily want to develop a whole voting system and put it through the certification process and everything. So I think it's not as much a cost savings although that's...

MR. SKALL:

But what does it mean? If I have a certificate for my component, what do I do with it? What does it mean? I guess that's my question.

MR. HANCOCK:

Well I mean you still have to have a system integrator.

MR. SKALL:

Right, so just a level of recognition that this component was doing what it's intended to too I guess.

MR. HANCOCK:

Right.

MR. GILBERT:

If I could address that on a specific basis, I mean I think that right now we have the paper trail requirement. This component of the electronic voting machine is tacked onto the machine. All it's doing is receiving data from the machine. Can't that be the kind of example we're talking about? I mean do we have to decide five different, you know, audit trail printers and stuff like that or can one manufacturer develop a really good one? But as you say, we don't have the, you know, the language standards, we don't have the structure, the database structure, you know, and all that. But that would be an example, Mark, of the kind of thing I think would fall into that category, wouldn't it?

MR. SKALL:

Well can I answer?

DR. KING:

Um-hum, sure.

MR. SKALL:

Again but what would be the purpose? So you have a manufacturer that does that, clearly he's not going to create a monopoly on the market so you're still going to accept other components that meet that objective, right? And you still have to test to make sure whether it’s delivered by that manufacturer or other manufacturers that it works together as a system.

MR. GILBERT:

Yeah.

MR. SKALL:

So again, my fundamental question is yeah, we’re creating some creditability for that manufacturer. Are we doing anything else -- we’re increasing the cost of testing it seems to me because now we have some specifications that need to be tested for individually, as well as, the system. I mean, you’re always doing that informant to some degree but typically you have the requirements and the standard and that’s what we’re testing for. Now we have additional tests and I’m just asking. I mean, I see where it may provide some use and maybe some costs and I’m just not quite sure what the goal is.

MR. GILBERT:

Well Mark, you could figure that.

DR. KING:

Okay. We do need to get moving on. Paul if you can very quickly address your issue and then Russ and then we’re on to Question 6.

MR. MILLER:

Okay. Well I guess the way I’m understanding this question now in this proposal, from an election standpoint, I think there have been times when certainly jurisdictions would have liked to have been able to purchase a component from one company and another from another company...

MR. HANCOCK:

Absolutely.

MR. MILLER:

...and that that would have been a helpful situation. I think in terms of being able to test that as a component and certify it as a component of election systems, we would have to develop standards for common interface as you suggested earlier and we haven't done that. And that would mean that we would require that all systems accept that common interface and that they utilize it.

DR. KING:

Okay, thank you. And Russ has deferred to the expediency of Question 6, thank you. Question #6 is something that's very specific. It says in the current draft of the VVSG are there things that need to be added or removed that we can be specific about and how could the process of developing and vetting the VVSG be improved to ensure higher volume and higher quality input from election officials? So that's two questions. I -- in the interest of getting on to lunch, I would like to hold this part to very specific suggestions as opposed to philosophical observations perhaps so, George?

MR. GILBERT:

Specifically, I think that Chapter 4 should be removed. Basing IVVR on manual counting of paper ballots has no standards, which can be applied. It doesn't belong in any kind of voting system standard when you're basically saying that this standard is based on something that we have no standards for. There's no way to document quality control. There's no way to document accuracy. There's no way to develop a standard for manual tabulation. Every even it is a unique event. And what we're doing in Chapter 4 is basing our whole backup, our testing, our foundation on something that can't be tested and can't be certified.

And I think the issue of having to accommodate interface is a very, very important area of standards that the EAC needs to pursue whether it can be done so in the context of this version of the VVSG I don't know but it certainly needs to go on the table. Thank you.

DR. KING:

Okay, thank you, George. Deb?

MS. SEILER:

Two things.

DR. KING:

Um-hum.

MS. SEILER:

One is I think it would be helpful for election officials to know what the time horizon is here and what effect these standards would have on existing systems just does this make them obsolete or not? You know, just what does it do?

And then the other thing that I -- that struck me in Part 1, Chapter 5, physical security requirements, it seemed like that needs to be reviewed. Some of those, perhaps many of those are actually I think the real purview of the election administrator rather than the vendor, the manufacturer. So I would just throw that out.

DR. KING:

The second thing you said, Deb, if you wouldn't mind repeating.

MS. SEILER:

Okay.

DR. KING:

Timetable for standards and...

MS. SEILER:

Was the timetable for standards and what the effect is on our current systems.

DR. KING:

Okay. Obsolescence of current systems, thank you. That's a beautiful thing. Well let's use our lunch break constructively because you may want to reflect back on this question and include these kinds of observations. I know Deb had already mentioned earlier that -- in the last part of this question how to get higher and more quality input from election officials may be to take advantage of state organizations and presentations of state organizations. So maybe we can think about some of those things over lunch and come back.

Lunch is on your own. There are the same fine coffee shops that I mentioned earlier also sell food. And we will reconvene here right at 1:00 and we will finish up by 2:00 today. Thank you.

***

[Luncheon recess from 12:04 p.m. until 1:00 p.m.]

***

DR. KING:

Let's resume. And I'd like to just kind of recap the agenda for the roundtables. The first part of the roundtable discussion this morning addressed the six questions that have been really presented to every roundtable so far and trying to collect the different viewpoints of each group on that. The remaining hour is now an opportunity for members of the panel to summarize their thoughts and reflect on what they heard and to make sure that as we put the transcript of this panel discussion into the record that the things that you think are most relevant and most important and should be deeply considered by the EAC that that gets addressed in this closing period. And the way that I would like to do this today is start with Keith and then we work our way around the table and we'll end with Brian as the host of the EAC here gives him an opportunity to make the final closing thoughts. And again, I'd ask you take, you know, somewhere between three and five minutes but if I hold up a finger, it means you've got about a minute left but we want to make sure that everybody gets their thoughts in.

MR. RAGSDALE:

Which finger was that again?

DR. KING:

I'll hold up a pen, how about that? And again if you have material that you've submitted in the written testimony, that also goes into the record so there's certainly no need to read from written testimony if you can summarize it in some other way. So Keith, if we could begin with you and then we'll work our way around the table.

MR. CUNNINGHAM:

Okay. Well first, you know, thanks for the opportunity. This was stimulating. I guess, you know, I don't know what I can add technically because, you know, again like I said earlier, I'm a little more of a practitioner than a technical technophile. I think that the

-- again, I focused pretty much in my readings and my continued readings on the usability issues and functionality issues that would concern me. So I think that the statements I made at the beginning about putting things into the standards that create expectations. You know, I think that we have -- we cannot look at these standards with all due respect to Mark, I mean, I think as a scientist he does look at them irrespective of the politics, but I think we have to look at them in the context that they're going to be applied. And we have to be careful not to create standards that do carry with them some degree of unrealistic expectation or some unattended consequence that local officials are ultimately going to have to deal with.

Having said that, it's certainly my hope that we will at some point, this has been a rough five or six years for all of us. And I certainly hope at some point when sooner than later we can get some mutually agreeable standards and these standards I guess locked down and in place and then, you know, begin with our assessment of whether or not the equipment we currently have is what we need and, you know, what equipment is on the horizon that will satisfy those standards, and who's going to pay for it, and what is the deployment scenario going to be?

I think, you know, I find myself a little frustrated, you know, as an official that has spent a couple of years deploying a new system that was supposedly up to snuff only to have a secretary of state come into office and, you know, want to throw the whole thing out the window and not have any real understanding of how long it actually takes to successfully deploy a system. We talked about that here today that there’s a certain level of maturity that comes over the years with a system. And this whole thought that a system can just be put into place and somehow magically the voters are all going to do it right and the poll workers are all going to do it right. And I guess that’s what I -- one of the things I would say the most is please understand that the amount of time that it actually takes a local election official to get a system in place, to get all of the necessary components up to speed, all the people that are involved with it trained and trained properly.

And I think the -- I’m very encouraged by the other side which is the EAC’s development of the management guidelines. The continuing need to professionalize those of us in the election administration business and give us the tools and give us the resources to be more professional and understand more about what we do is critical. So I know that’s not part of the -- and I would hope that at some point, we can do something that has a few less acronyms associated because I can’t keep up with all these. I had to bring the book with me to remember what they were.

So I hope my presence here today has been helpful, thank you for the opportunity.

DR. KING:

Okay, thank you, Keith. David?

MR. DRURY:

Thank you. I guess I have several areas that I’m concerned with in regards to a stable voting system as opposed to for -- I guess from my perspective we have to continue to improve, continue to improve that, expanding upon that. If we have a system that’s stable that doesn’t have continuous improvement, it’s a concern to me. If we would consider perhaps maybe an addendum or something of that nature. Again, my perspective is that changes are going on in this state. In particular alleg (ph) image capability and as I mentioned before the ballot box issues and getting rid of the ballot box converters and that sorts of thing. So, anyway, that’s one area that I’m looking at.

The other area is the component test. Pretty much like Mark was saying, why? These counties, again, I’m only with Florida. These counties are concerned about the cost and having additional risks with an election and having different vendors involved in the voting system is a great concern. Not only do they have the costs, the contracts, the maintenance, and if you have a failure during an election who’s going to have responsibility? Those are concerns. And a lot of these counties are continuing with their Legacy Systems.

I also have a few issues about open-ended vulnerability. I would like to see if -- and there’s nothing wrong with it but it’s the time frame. If we’re going to have an open-ended vulnerability test, I’d like to see it done before certification testing not after. Those are basically my thoughts.

DR. KING:

Okay, thank you, David. Lowell?

MR. FINELY:

Every day in my office I get an internal email with the attendance and then there’s a little thought for the day that changes each day. And since it’s three hours time difference that came in during lunch.

And today it was is it possible to be totally partial? And I liked mulling that over. And I think the one thing that I come away from this meeting with is that it turns out I don't think any of us are totally partial. I think we've actually found some common ground. I detected a couple of things that we've agreed on, George, even after you had given me your...

MR. GILBERT:

Coffee.

MR. FINELY:

Well that's a starting point. But in terms of specific issues we've discussed, I think on the risk assessment question, I found Mark Skall's comments to be very helpful there in terms of moving away from the emphasis on quantifying risk and recognizing that the principal value of the exercise is for all the stakeholders in this election and voting enterprise to get together and have the discussion about what the range of risks is and what are the known mitigations. Just that process itself I think is a useful one. I just again express my concern that we don't delay implementation of vastly improved standards while we conduct that study. And again the climate change debate comes to mind.

On open-ended vulnerability testing, first I want to withdraw the two new acronyms that I proposed today out of difference to my colleague. You'll never have to use those. I'm sure that you weren't really planning to anyway. But I think open-ended vulnerability testing is necessary but not sufficient. I think it really is critical to have that as part of the certification of voting systems. But as I think a couple of people have commented, you can't guarantee through testing that a system is safe and will operate correctly. And you also can't guarantee that you have identified all vulnerabilities and possible attacks. In fact, the experts we've worked with stress that every time we talk to them and every time they write something up. So I think I agree with many on the panel about the importance of knowing what the vulnerabilities and risks are or at least their broad categories and then working on the mitigations that will help in addressing those. In my view, it took a few years for the procedures and mitigations in place to catch up with this new technology. I think we beta tested a new technology in the field with, you know, presidential elections and I think that's unfortunate, but I think we're actually moving in a positive direction.

I also thought that Mark's comments about one of the potential problems with vulnerability testing being achieving uniformity across labs in terms of the quality of the inspections is an important issue and, you know, Mark spoke about one idea of creating cross firm teams to do this. I would also suggest that it's important periodically to introduce new blood into the process. And I think that computer science graduate students who are specializing in security are really an ample, you know, a resource that should be taken advantage of both in terms of keeping down the costs of doing this but also getting the latest in terms of what's being studied and learned in the academic setting.

Standing back and just looking at the VVSG generally I think that the work that NIST and the TGDC have done is really excellent. I think the proposal that they put forward is a very strong document. And I think it's important that we continue this process of public feedback, feedback from the various groups but move and at that all deliberate speed toward adoption of these standards and also to relatively prompt enforcement date for those standards.

I think one thing that is sort of unspoken here but is true is that the vendors have a pretty good idea about what's coming and what they're going to need to be designing to. And I think they're probably already working on that. And when you add to that the incentive of wanting to be the first out of the gate with a system that's certified to new standards, I think we shouldn't be too concerned that we'll be getting out ahead of the technology.

And that's the key points I would like to conclude with, thank you. And I also just wanted to thank you, Merle for being such an impartial host of these discussions. I think you've really done an excellent job. And I express my appreciation to Commissioner Danetta Davidson and the other commissioners who sat in for parts of this because it's important to hear it and not just leaf through a transcript at some point later on. So, thank you.

DR. KING:

Thank you. George?

MR. GILBERT:

This morning I suggested removing Chapter 4 o f the VVSG and like Lowell I wish to make a withdrawal of the previous proposal. I withdraw the request to remove Chapter 4. Obviously security and audit standards are fundamental to voting systems. The problem that I encountered in Chapter 4 was its integration with the concept of software independence and its reliance on manual tabulation and paper audits. I have raised this issue at every forum I have participated on this subject, but I raise it again. When NIST can tell me how they're going to guarantee the accuracy and integrity of manual tabulation or manual audit systems based on paper, I will be happy to listen. Thus far, no proposal has been forthcoming and no suggestion as to how it might be done has been forthcoming. I strongly favor IVVR's. For Keith's benefit, that's independent voter verifiable records.

MR. CUNNINGHAM:

I was about to look that up.

MR. GILBERT:

I think that having the IVVR concept is critical to the future of elections because it's critical to the future of electronic tabulation and the security of electronic tabulation, which is what we are going to have to use for most of our elections and most of our tabulations given our population. However, if the software independence standard also applies to the IVVR's, you are left with nothing but paper records to rely on.

The concept of electronic monitoring and auditing, independent electronic monitoring and auditing of systems is not a new concept. It's used all over the place. And it seems to me that we do not have to wait until there is a market ready electronic audit system in order to write standards for such a system. If you have to wait until there's a market ready when -- and you apply the software independence standard, you will never get one. And we will never have a firm foundation for ensuring the integrity and accuracy of our tabulations. That's all I have to say. I don't want distract anybody from that thought.

DR. KING:

Okay, thank you, George. Paul?

MR. MILLER:

I'd love to respond to George's comments but I will not at this point. The -- and since I don't want to repeat what other people have said well, I want to address up front an issue that hasn't been discussed quite as much. I probably alluded to it several times and that's the issue of cost. There's no question that the volume testing, the standards themselves in terms of how they assume what the manufacturers have to is going to increase the cost. That's not necessarily a bad thing but when you combine that with the lack of clear funding sources for that, then there -- I think there is an issue.

I would love to see the Congress and obviously that's outside of our area of what we can actually do something about, but I'd love to see Congress pass something that would tie funding for the jurisdictions with this release, with the release of these standards. If we look at the industry as a whole, I think that what we've seen are actually relatively small companies developing these systems. They've known that there wasn't a terribly large amount of money available and it was a long cycle. The funding cycle was a long period of time and then suddenly HAVA poured in a lot of money in an industry that wasn't prepared to handle that money. So what I'd like, what would be ideal from my perspective would be funding that is clearly tied to a cycle that the vendors can respond to that's tied with the standards.

And in all of this and in doing the volume testing and in doing the open ended vulnerability testing, I have a concern that we keep in mind that -- and it isn't that I want to fool the public, but I want there to be an accurate perception of what is really happening with these tests and what is really -- what we really are finding out. We operate in a public arena. A lot of the stuff that -- a lot of the problems with systems that have been well publicized are real problems and they are vulnerabilities, but in almost all the cases with a few exceptions, we have been handling those with -- procedurally. The systems, you know, I will freely admit that the systems were not designed back in the 1995's when nobody was thinking about security and hackers and including Microsoft and everybody else needed to be upgraded. But as we look at these issues, I think we also need to take into account when we do open the procedural processes that election officials use.

DR. KING:

Okay, thank you, Paul. Russ?

MR. RAGSDALE:

I'd like to use my twenty minutes to address -- well I'd like to take a shot at that last part in the last question we didn't get to. How to ensure higher volume higher quality input from election officials? And what I'd like to do is propose an idea to the EAC. I'm sure it's not a novel idea nor an original ideal, we barely have either. I'd like to see the EAC put together a road show, a presentation. I think Debra, you mentioned earlier there are state conferences around the country of election types that occur. We're a very social animal by nature, I think. We do have a tendency to pack up and go to opportunities to deliver that message. Get out in front of these folks, engage them, explain what the VVSG is what the development process is, why the VVSG is, more than anything why it is.

I encounter my peers on a regular basis that really don't understand the purpose of the VVSG and it's hard to try to explain the operations of the VVSG if they don't know why it's there. I think that if the EAC is lacking in the resources to get out to the 50 states and territories, aggressive action or standards board members and advisory board members, I'm sure you have folks on those that would be more than willing to deliver those presentations out to their respective communities.

Again, bear with me. Take that trip to the eastern plains of Colorado again. If I'm a clerk in a small -- I'll take this opportunity to voice my perspective from a small jurisdiction. If I have to appear in front of my budget authority and I'm in this small county out in the eastern plains of Colorado and I've got 2,000 voters in my jurisdiction, and I'm asking the budget authority for the amount of money to buy my system that they equate to the same amount to buy a snowplow and a couple of emergency vehicles, how do I make that case? Help me do that right, wrong, or indifferent, give me the tools to be able to do that. I think the EAC -- it's incumbent upon you to do that, to get that message out. And you may not have to do it yourself. I think as a member of the standards board, I'd be more than happy to volunteer doing that presentation in Colorado. I'm sure you'd have the same level of volunteers around the country with other members, too. So, that's it. And my other two minutes, I want to concede to Keith because I don't think he was done.

DR. KING:

No, I think Keith is done.

MR. RAGSDALE:

He's done.

MR. CUNNINGHAM:

I didn't hear the last part, what did you say?

MR. RAGSDALE:

I was giving you time.

DR. KING:

Thank you, Russ. Okay, Deb?

MS. SEILER:

Well my confession...

MR. CUNNINGHAM:

At least he didn't say the gentleman from Ohio.

MS. SEILER:

Well my confession to the gentleman from Ohio is it might be helpful to put that table of the acronyms up in the front of the document. I found it in the back...

MR. SKALL:

No, we don't want to make it too easy.

MS. SEILER:

Yeah, okay, all right. I do appreciate -- first of all, I appreciate the opportunity to be here. I appreciate the standards project. I appreciate the fact that it's been going on for these now decades, I guess we could say and that people are still devoted to it. I think there are some very positive aspects to it. I was very happy to see, although we didn't touch on it too much but the reliability and this issue of volume testing that I think is important and it was lacking as, you know, some of these new systems were coming into being so I think that was great, a great addition. And there is a lot of thought, a lot of work has gone into it obviously and I appreciate that.

I don't know if I share Lowell's optimism about how feasible some of these things are. I just don't have maybe the knowledge of the industry. I hope it's feasible. I hope they can -- these things can be accomplished in a cost effective way. I very much do.

I'll reiterate the fact that I do feel the election officials need some education in all of this. It sounds like, you know, a starting point has already been laid down. I would hate to see us get to a point where election officials really can't talk to their IT people on these matters. Where we just -- where election officials just say oh, give that to the IT people and trust them.

I think election officials need to have some working understanding of these standards and the management implications that they have for our operations. I think election officials also have an opportunity to provide a tremendous amount of input into the whole aspect of risk assessment and not so much from an engineering standpoint but from a kind of a real world perspective. Wee sort of have a crisis of confidence and voter confidence, I think in elections. I'd like to see, I'd like to hope that these standards would help us overcome that. I think we need to be dealing with real issues, real threats, real risks, rather than perceived ones and to the extent that the EAC can help us sort of defying between what are the real threats and what are the perceived ones I think that that would help us restore that confidence.

I would join Russ in inviting Mark, the EAC, anybody out to California. I think that, you know, we would love to have you come out and speak to these issues so.

And I think my final point is that I would hope that the states would once these standards are adopted, would really adhere to them and not be going off in different directions or taking matters into their own hands and would really stand behind these.

DR. KING:

Thank you, Deb. Mark?

MR. SKALL:

Thank you. Yeah, a meeting in California perhaps on the beach would be...

MS. SEILER:

San Diego in 2009 you got it, we'll be there.

MR. FINELY:

No, it wouldn't have to be in one of the eastern plains counties. We have them too.

MR. SKALL:

I also want to reiterate the thanks to Merle and the EAC. You know when you've done these five or six or seven times and you keep thanking people all the time it sounds old and the last time I thanked this many people I think was at my Bar mitzvah. It's well deserved. I mean these are really good forums. The exchange is great. We get differing opinions and we talk about them civilly and hopefully we learn from each other. So I think it's been a really good experience.

The challenges in voting, I think are really great. We at NIST have worked many, many fields of IT from electronic commerce to database systems to healthcare IT standards and I'll tell you, voting is unique. The rest are just pieces of cake compared to this. And there are many reasons. The secret ballot, this crazy concept of the secret ballot causes a lot of these issues. If it wasn't for that, this would be a lot easier but I guess we'll stop at that. And of course the public scrutiny and the process it's a very challenging area. Couple that with the state of the art of software testing that you cannot prove an implementation is correct, you can only prove it's incorrect leads us to many, many challenges and hard decisions to make.

So the first thing we have to do is clearly develop a very good comprehensive standard. And I've heard Keith talk about unintended consequences and I think we may only need to have a couple of drinks and talk about this because I'm still not exactly sure what you mean, but if what you mean is being able to read the minds of critics, politicians, and what people are going to say based on what we do, I just ain't that smart. I mean, I just don't know where to start. So I think what we have to do is really write the best technical standard we can. We will address those concerns when they come, we will answer them, but I don't think you could guess at what people are going to say and how they're going to misuse what you do. So I think we have to do the best job we can to from a technical standpoint to develop this.

I think software independence has been brought up is a necessary evil if you will because of the fact that you cannot associate a voter with the transaction so it's very, very hard to get any closure. You don't know when errors are created, you don't know when transactions were done incorrectly. So it's very, very difficult and the fact you cannot prove that the software is correct, you need some mechanism to be able to audit the systems inability and that's when software independence comes. I agree IVVR defaults to paper and that is, you know, perhaps unfortunate. I don't think any of us and I'm guessing Lowell as well love paper. I don't think any of us love paper. It's a necessary evil. We know the problems with paper. We're all aware of that. Unfortunately in the standard you can talk about software independence at a very high level and leave it at that in which case it's completely non-testable and meaningless. Or you can bring it down to a lower level and the only way we know how to do these audits now is through paper. We do have hooks in the standard through the innovation class where we hope to have ways to do this more, in more what it needs and that is the reason for the innovation class primarily. So we do see a way out of that but right now we have what we have.

Risk assessment again needs to be multi-disciplinary. And again, I would just say we can't have really high expectations that this is going to be the end all and be all. We have to use it in the context of, you know, I hate to say garbage in, garbage out. Basically the numbers we put in are going to determine the numbers we get out and they are really subjective numbers.

OEVT, I agree with you, Lowell that the name is just horrible. And I said yesterday if we had to do it over, I don't have your very nice acronyms, well just all it expert system testing or something like that. It gives a bad connotation and perhaps inflames the community. It is something I think needs to be done and again whether it's done within the standard context or somewhere else is not that important to me as long as we assure it's done.

DR. KING:

Okay, thank you, Mark. Brian?

MR. HANCOCK:

Thank you, Merle. And we certainly appreciate the thanks from all of you but really it's us that should be thanking those of you at the panel...

MR. SKALL:

That's right.

MR. HANCOCK:

...because you've taken your time, not you. Taken the time away from your election official duties in this election year and have come all this way to Washington to share your thoughts with us and we really sincerely appreciate it. And we hope you continue to do so as we go through this process. I know a lot of you have provided us with your written testimony, but if there are any other thoughts in any other details, you know, there's a lot of depth to this document please comment to us via our web comment tool by May 5 because we need all the help we can get quite frankly in this.

And once again, I just want to thank Merle as well. I agree with all the sentiments here that he's done an excellent job moderating many different groups of people over the past several months and thank you, Merle.

DR. KING:

Thank you, Brian. I'd like to make a few summarizing comments, but the first one I was thinking, Deb that at the pace we're going, we can probably get to all 50 states to do the road show if we do two a year and still bring this thing in within our lifetime. California would be...

MR. HANCOCK:

Labor of speed.

DR. KING:

It would all be at deliberate speed. What I like to do at the end of each of these mostly for my benefit but also as a way of recognizing and kind of reflecting back on just how much ground we have covered in four hours today is to go through my notes and share those observations with members of the roundtable.

Some of the things that I heard today was that looking for a consistency of readability in the standard would be a desirable feature. The development of road show of seminars to move the VVSG not only in its current version but also the implications for the management of the VVSG should it be adopted within the jurisdiction. That we cannot engineer all requisite security into systems through the VVSG and that there will always be a need for attention to implementation of details. That the cost associated with mitigating risk are also a necessary part of the risk assessment that as we begin to implement mitigation that introduces its own risk and uncertainly at times. That a risk assessment should not unduly delay the adoption of the VVSG. That risk assessment is essentially an assessment of electronic voting in the system and that the risk assessment needs to broaden across the paper elements, the physical elements, as well as, the electronic.

That the system that comes out of the VVSG may exceed the performance capabilities of the poll workers that are responsible for managing and implementing these procedures at the polling place level. Risk assessment should be a comprehensive balance across the spectrum of the scope of the system as opposed to specifically identifying. That perhaps one way of simplifying the standard to a point of improving it's readability is to use a non-quantitative a three tiered rating system that may provide an understanding without the burden of quantification. That risk assessment should be an ongoing process rather than a one-time event.

That the customers of the voting systems have demands and those demands may drive us towards more short-lived standards. That the standard perhaps can be both flexible and stable. That if there are methods within the standard to accommodate innovation and flexibility it may be possible that we can derive the benefits of stability, as well as, flexibility. Component testing would permit needed and required changes perhaps, statutory changes or innovations mandated from some other source to be adopted and implemented as needed. That we need to define standards for a common interface to support that component testing. That there should be a timetable published for the implementation of the standard and specific addressing of its impact on existing systems.

There are things perhaps in the standard that create expectations and if these are unrealistic expectations there may need to be accompanying documentation to help articulate how the standard accurately changes current systems without creating unrealistic expectations. The amount of time that it takes to get a system on line and smoothly operating argues for deliberate consideration of the standard. That continuous improvement is a desirable attribute of voting systems management and that the standard should reflect the scope, the ongoing continuous improvement philosophy. The time frame from OEVT should precede certification of a system. The principal value of the risk assessment process maybe imparted in the dialogue itself as a opposed to the metrics that come out of it. The OEVT is a necessary function, a necessary feature of the VVSG, but in and of itself is not sufficient, does not replace good design of a system.

The need for consistency in all forms of testing whether it's OEVT or the routine testing at the labs is an important consideration. We should review the extent to which the components of the VVSG interact with each other and with an eye to completeness and consistency within the sections of the VVSG. That an increase in cost is an understandable consequence for expanding the scope and the rigor of the standard but explicit and implicit costs of the standard must at some time be addressed. That the outcome of the OEVT needs to be accurately and contextually presented to the public. That a road show of the

VVSG process, the why we have the VVSG, the what it is, and how it will be implemented is a desirable outcome.

That we need to provide election officials with the information to make the case to their funding agency boards and other constituencies about the value of certified systems. That election officials need to understand the management issues that are associated with the standard of the systems derived from it. Election officials need to be involved in the risk assessment. And finally, the consensus and the support of states in the concept of a federal standard is a desirable point.

So those were the things that I heard today from the group and I hope I've captured the things that...

MS. SEILER:

Pretty impressive.

MR. CUNNINGHAM:

I didn't think you were listening that close. We didn't even know we said all that. That's good.

MR. MILLER:

May I make a comment that I would like to also extend my thanks to Merle for moderating that and not only summarizing very well what we talked about but making it sound smarter than we are. Thank you.

DR. KING:

Thank you, Paul. Again, this has been the sixth in the series and we have ended every one of these on time and today will be no exception. So again, I thank everybody...

MR. SKALL:

And it’s early, too.

DR. KING:

...for your travel and your contribution and your efforts in this regard. Have a great afternoon. Thank you.

***

[Whereupon, the roundtable discussion adjourned at 1:44 p.m.]

COMMONWEALTH OF PENNSYLVANIA
Department of State

U.S. Election Assistance Commission

Written Testimony of Kathleen M. Kotula
Director, Office of Policy
Pennsylvania Department of State

April 25, 2008
Washington, DC

Public Discussion of Voluntary Voting System Guidelines

Chairwoman Rodriguez, Commissioners of the U.S. Election Assistance Commission (EAC), and distinguished members of the discussion panel:

On behalf of Pedro A. Cortés, Secretary of the Commonwealth of Pennsylvania, thank you for the invitation to participate in the roundtable discussion of the proposed next iteration of the Voluntary Voting System Guidelines (VVSG). We welcome this opportunity to provide written comments in response to the discussion questions.

The Pennsylvania Department of State (Department) is committed to holding fair, accurate and accessible elections. Election administration in Pennsylvania occurs at three levels – at the state level by the Secretary of the Commonwealth who serves as the Commonwealth's Chief Election Officer, at the county level by the elected county commissioners or other legally established body, and at the precinct level by the elected and appointed district election officials.

Pennsylvania has sixty-seven counties that range in size from small rural areas to very large urban areas such as the county of Philadelphia. There are over nine thousand two hundred precincts in Pennsylvania.

In Pennsylvania, electronic voting systems must undergo a statutorily required testing process. The system must be tested by a federally recognized independent testing authority. Then, unlike some states that only require the federal testing, Pennsylvania law requires a second tier of testing. The state testing is conducted by an independent testing examiner. After successful results of both testing processes in Pennsylvania, the Secretary of the Commonwealth certifies the system for use in Pennsylvania. Counties then select the system that they will use from the list of certified systems.

Currently, there are twelve types of electronic voting systems certified for use in Pennsylvania. In Tuesday's general primary election, ten of those electronic voting systems were used throughout the state, including six direct recording electronic (DRE) systems and three optical scan systems. DRE systems are the most prevalent electronic voting system in Pennsylvania, with fifty-five counties using such a system. Optical scan voting systems are used in sixteen counties.

It has been suggested that DRE voting systems in Pennsylvania should include a voter-verifiable paper record (VVPR). Indeed, this next iteration of the VVSG seems to require such a feature to meet the definition of software independence, unless the voting system falls under the innovation class. The Department has certified four optical scan systems which provide a VVPR. It is important to understand that the Department is not opposed to a DRE voting system with a paper record capability. The issue to date, however, is that the Department has yet to examine a DRE voting system with such a feature that meets state constitutional and statutory requirements. Both the Pennsylvania Constitution and the Election Code provide that a voting system must preserve the fundamental premise of secrecy in voting. A mechanism like a continuous roll VVPAT as it exists in the marketplace today violates this secrecy requirement. The ballot images are recorded on paper in the order in which they are voted. As such, a person only has to compare each ballot image with the numbered list of voters maintained by district election officials to reveal each voter's selection. The numbered list of voters is public information that is available to the public for inspection upon request.

Moreover, the other question that arises in Pennsylvania with this type of voting system is which vote should be counted in the event of a recount, the one recorded or the one printed.

These are issues that must be taken into consideration in Pennsylvania. The purpose of this background is to provide the framework and the perspective from which state election officials in Pennsylvania are analyzing and assessing the next iteration of the VVSG.

Voting system integrity and security is critical. In addition to the certification process, specific procedures are in place in Pennsylvania to ensure election system security. The systems are well secured and the counties have a specific chain of custody that designates authorized individuals to handle the machines before, during and after the election. Holding successful elections in Pennsylvania is a result of many factors.

With that background as a foundation, the written comments for the discussion questions are provided below.

1. *The VVSG has more than one audience, including vendors and VSTLs. Do you consider county and state election officials as one of the stakeholders in the VVSG and therefore one of the intended audiences? If yes, is the document intelligible to you? If not, how could it be improved?*

County and state election officials are certainly stakeholders in the VVSG and should be considered intended audiences. Overall, the document is intelligible but it is somewhat difficult to navigate. For example, acronyms are used repeatedly throughout the document, which causes a reader to constantly refer to the glossary. Within the glossary, the definitions build upon one another and that means there are definitions within definitions. The need to constantly refer to the glossary section can easily distract the reader's review of the underlying requirement.

The document is extremely lengthy. The concern with a document of this length is that a reader may not be inclined to read the entire document. The length also makes it cumbersome when the reader needs to find a particular section quickly. Moreover, the document's language is geared towards its primary technical audience. All of these aspects together could potentially limit the amount of feedback that the EAC will receive from the various stakeholders at large.

It is important that the guidelines provide standards that are able to be met by the vendors and that are capable of being implemented at the state level. In Pennsylvania, our state certification process builds upon the testing that occurs at the federal level. As such, it is critical that we are able to understand the requirements of the document. The requirement for software independence is an example of such a concern. It would be useful if software independence was defined even further in the VVSG. For example, there should be some indication as to what the critical steps are that a vendor must prove for a voting system to be deemed software independent. There is a concern that if the standards are unreasonable, the vendor community will be deterred from incurring the cost to move forward with an innovation.

2. What are the essential elements of a risk assessment? How can the EAC best create a risk assessment that recognizes all possible risks and assesses the plausibility and nature of such risks in an election environment? How do you evaluate what is an allowable level of risk?

A risk assessment must be properly grounded in theory and based on practical threats to voting systems. A risk assessment is probably better performed at the implementation level for the voting system, not necessarily at the federal level. In order to properly evaluate an acceptable level of risk, the process and procedure at the implementation level that surround a voting system must be taken into account. In Pennsylvania, we do not believe that potential risks to a voting system should be viewed in a vacuum. Rather, the entire security process that occurs at the county level must be considered. For this reason, we believe that risk assessments are more appropriate at the implementation level.

3. Could you comment on the value of stability in the standard to your jurisdiction? Which is preferred, a standard with a short-shelf life that accommodates innovation and change or a stable standard that may discourage innovation, but creates longer certification lives of voting systems?

Stability is important in Pennsylvania, but so is innovation to an extent so long as it is not cost prohibitive to the counties. The best solution is probably a combination of both standards. There should be general standards that are stable and do not change over time, but then there should be other innovation pieces with a shorter shelf life that are incorporated into the overall general standards.

4. What is the value of the open-ended vulnerability testing (OEVT) model? Would the current OEVT requirement in the standard reduce or decrease voter confidence in your system? If the EAC were to require OEVT how could it best be included into the EAC's Testing and Certification Program?

OEVT could be useful to test for some perceived vulnerable aspects to voting systems. However, this requirement should definitely be expounded upon in the VVSG. For example, the range of testing should be further explained. Depending on the type of testing, there is the potential to actually decrease voter confidence. A broad requirement of this nature could translate into the belief among voters that the testing is necessary because the systems are inherently untrustworthy. If OEVT is included into the testing program, there needs to be an assessment as to what length of time this testing will extend the federal testing process. This is already a somewhat lengthy process from start to finish and this type of testing has the potential to extend that time even more.

The results of testing and threat vulnerability should be disseminated to county and state election officials. Access to this information is important to Pennsylvania's certification process. The VVSG should clearly outline how and when the results of OEVT testing will be made available. Moreover, county and state election officials should have access to the actual OEVT report, not just a condensed report.

5. Would component testing (the ability to test and certify components as they are modified or added to an existing system) be beneficial to your jurisdiction?

Component testing would be beneficial to Pennsylvania. The fact that a vendor must submit the entire voting system to testing once a modification is made tends to increase the amount of time for testing. Component testing would seem to streamline the process. However, this should be limited to some extent. There should be a benchmark that if a certain number of components are changed, then the entire voting system must be submitted for testing.

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? What needs to be added or removed from this document in order for it to meet what is needed from future voting systems? How could the process of developing and vetting the VVSG be improved to ensure higher volume and higher quality input from election officials?

As mentioned, this is a rather lengthy document. In comparison, the companion guide is relatively short. A guide that is somewhere in between these two documents may prove useful. The target audience for the guide should primarily be county and state election officials. A less intimidating document would most likely result in more feedback to the EAC from the stakeholders at the county and state levels. Feedback from a larger sample of stakeholders will result in more complete standards.

The EAC should consider streamlined presentations at various meetings of the National Association of Secretaries of State (NASS), national organizations for state election directors, and at various county level conferences. This broad range of feedback will be beneficial and contribute to the overall practicality of the standards.

Election Officials Roundtable

Friday, April 25th, 2008
EAC Offices
1225 New York Ave, Suite 150
Washington, DC 20005

Discussion Questions
(With Comments by George Gilbert in red.)

Voting systems manufacturers today must design their products to fulfill a broad and ever-expanding list of requirements to meet the needs of an increasingly diverse voting public, while at the same time attempting to provide an efficient and cost effective product for election officials. Election administrators place additional value on other attributes of a voting system including ease of system setup, operation, and maintenance; configuration simplicity; reliability of operation; processing accuracy; ability to audit entire process; and high polling place throughput. The demographic makeup of the voting public itself also influences voting system design to a great extent. These demographic factors include age, educational level, language proficiency, manual dexterity, physical mobility, sensory functioning, and commuting distance from polling place. Finally, and perhaps most importantly, voting system design must also mitigate a variety of potential threats to the voting process.

The voting system design process needs to take all these factors into consideration and strive to strike an optimum balance. This is a difficult task because many of these factors conflict with each other. As the scope of requirements increases, satisfactory solutions become harder to define. This is an environment where the design process must be open to innovative approaches and unbound by technological constraints so the very best solutions can be implemented in a timely manner.

The next iteration of the VVSG will dictate the direction of voting system design for the next generation of voting systems. The challenge for this next iteration of guidelines is how to properly balance the need for improved security, audit ability and accessibility while also creating guidelines that are not so prescriptive that they stand in the way of innovation. Technology in and of itself has a neutral value scale and can only be evaluated in the context of its application. A voting system is an information processing system. The historical trend in information systems technology has been to supply ever greater capabilities with simpler configurations at lower cost. Information processing has moved from paper and electro-mechanical devices to fully electronic processing and from a host of special purpose devices to general purpose devices.

As the issuer of these guidelines the EAC has a duty to examine these proposed guidelines and decide what the next generation of voting systems must be capable of. Two of the driving forces behind the suggested security requirements in the TGDC draft VVSG are concerns about the integrity and trustworthiness of electronic voting systems and the difficulty of verifying that software only does what it is intended to do and does not harbor malicious code.

The 2007 VVSG recommendations introduce a number of design requirements and validation concepts for the purpose of improving the security of voting systems. These recommendations constitute a radical change from previous voting system standards. These concepts include Software Independence (SI), Independent Voter-Verifiable Records (IVVR), Open Ended Vulnerability Testing (OEVT), and usability benchmarks. Each of these will introduce additional complexity to system design and development and therefore increase the cost and risk for vendors. And all except OEVT will impact voters through changes in the voting process itself. The concepts of Software Independence and IVVR offer additional security but also lead to concerns as to the accessibility and usability of the voting systems.

Before imposing these changes on the election community, it is the EAC's responsibility to determine the best means for providing a sufficient level of voting system security without requiring disproportionate tradeoffs against other highly desirable voting system features. To this end the EAC is convening roundtable discussions for the purpose of carefully considering the VVSG recommendations. This discussion will be conducted in six segments:

1. The VVSG has more than one audience, including vendors and VSTLs. Do you consider county and state election officials as one of the stakeholders in the VVSG and therefore one of the intended audiences?
   Are members of the armed forces stakeholders in the war in Iraq?

If county and state election officials are not among the VVSG stakeholders, then it has none. County election officials are the primary stakeholders in the VVSG. As voters, we have a common and equal interest with every other voter in the security and integrity of our voting systems. As the election administrators, our entire careers are at stake. Our ability to perform our jobs is at stake. Our personal reputations are at stake. The VVSG determines the options available to election administrators in carrying out their duties.

   a. If yes, is the document intelligible to you?

Parts of it. It is, however, too expansive, far too detailed, for the vast majority of election officials, including me, to even read much less comprehend. I seem to recall that the cross referencing, at times, required multiple readings and, more than once, resulted in new interpretations of what was being stated.

Of the parts I have been able to read, most is "intelligible," and cause for great concern. One example is represented by Part 1, Chapter 7.5, "Casting." After reading:

> "The requirements in this section mandate that privacy of the ballot be protected throughout the entire process of credential issuance and ballot activation, and that **no information be maintained in reports or logs that could assist in identifying a voter's cast ballot (except for provisional voting on a DRE)**,"
> (emphasis added)

the conflict this presented under North Carolina law made it difficult to assess the entire chapter. (NC law requires all "absentee" ballots to be identifiable and retrievable.)

(Further examples of these concerns I have addressed in my comments and will not repeat here. A copy is attached for those who are interested.)

b. If not, how could it be improved?

The "performance standards" assumed in the VVSG go well beyond those required to accomplish the objective, eg., as noted above, in specifying too far reaching a "privacy" standard. Further, they delve into specifying HOW these performance objective must be met.

Perhaps most troublesome is the apparent attempt to eliminate all possible technology based threats to the voting systems while ignoring the human threats, eg., the inevitable errors or mischief inherent in manual handling and tabulation of paper records.

A more effective approach, and far less expensive, would be to recognize that "voting systems" are not simply equipment. Voting systems are equipment and procedures associated with the deployment of that equipment. While this may place the technical folks in what they feel is an "ambiguous" position, the purpose of the VVSG's is not to enable the folks at NIST to sleep well at night. The purpose is to enhance the accuracy and security of elections. Technical standards, no matter how detailed and tightly specified, cannot close the human loophole in real world elections, threaten to stifle innovation and threaten to drive out of reach of many jurisdictions the cost associated with implementing the technology. I understand that NIST is technology oriented. The EAC, however, must take a more holistic view of "voting systems." Elections does not need a "fail safe" technology. It needs reliable equipment that can be efficiently employed through good management.

2. 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.

a. What are the essential elements of a risk assessment?

Some thoughts:

All conceivable threats are possible (plus some that are not conceivable.) but few
have a high risk

"Risk" includes the likelihood of a threat being realized.

"Risk assessment" should be accompanied by cost-benefit analysis.

Who has a vested interest in disrupting or redirecting the outcome of an election?

Who with a vested interest potentially has the means to carry out their disruption or redirection?
What are the costs (including the costs of being caught) of executing such a threat?
Are the benefits, to those attempting to disrupt or redirect the outcome of an election, greater than the potential costs?

Is the means available on a widespread or limited basis?
Is there a history of activity that indicates that an attempt will be made to carry out a potential threat?
What measures are in place to detect or deter such activity before its culmination?
What are the weak points in such existing measures?
Who has the means of exploiting those weak points?
What measures can be put in place to detect or deter exploitation of those weak points?
What are the costs (including management and functionality costs) of putting such measures in place.
What are the benefits of detecting or deterring such potential threats?
What is the likelihood that the results on an election would be changed as a result of successful execution of the threat?

b. How can the EAC best create a risk assessment that recognizes all possible risks and assesses the plausibility and nature of such risks in an election environment?

It cannot.

However, as a starting point it can dispatch teams to participate, from the beginning, in local elections offices and take notes. Election officials, precinct officials and voters can create "threats" that no one could possible imagine or anticipate. Point out the threats you identify and then talk to us about how these threats can best be mitigated. Consider both changes in technology and management procedures.

The greatest threat to the integrity of elections in 2008 is the multiplicity of directives and devices for threat prevention with which election administrators are being enundated.

c. How do you evaluate what is an allowable level of risk?

Not allowable: Significant[1] undetectable error in vote recording
Not allowable: Significant undetectable error in vote tabulation
Not allowable: Unrecoverable loss of CVRs (cast vote records), including paper ballots

Allowable: Imperfect management that is not "significant"

[1] "Significant" is essentially defined by NC law as a large enough error to "materially affect" the outcome of an election with respect to a specific contested contest. Obviously this is potentially one vote, however, the likelihood of one vote being "significant" is very small.

Allowable: Voter error that is not "significantly" exacerbated by the voting system

Allowable: Irregularities that are not "significant"

3. Could you comment on the value of stability in the standard to your jurisdiction?
   a. Which is preferred, a standard with a short-shelf life that accommodates innovation and change or a stable standard that may discourage innovation, but creates longer certification lives of voting systems?

This depends on the quality of the certified voting system at any given point in time. If the cerfitied system is a good one, stability is certainly preferred. If it is not a good one, standards that facilitate change and innovation are preferred.

This leads me to the conclusion that the standards themselves should be structured to accommodate either situation. Systems working well should not be forced to change. For systems not working well, technically or in the judgement of the users, the standards should enable rapid and efficient modification. It should be as clear as possible that any set of standards establish a target for incremental change, not an absolute standard of accuracy and security.

4. What is the value of the open-ended vulnerability testing (OEVT) model?
   a. Would the current OEVT requirement in the standard reduce or decrease voter confidence in your system?

Would likely have no effect on voter confidence. Voter's tend to trust or distrust people more than systems. If they are confident in their people and processes, they will likely be confident in their voting system. Further, they will neither know nor care to know what OEVT is. That doesn't make OEVT a bad or useless idea, but it would not likely affect voter confidence.

   b. If the EAC were to require OEVT how could it best be included into the EAC's Testing and Certification Program?

OEVT should not be included in the VVSG as a comprehensive "pass/fail" set of standards. There is a high likelihood that any "system" could "fail" the test criteria at some juncture but remain a viable voting system within the context of an acceptable risk assessment model. Further, management procedures can frequently be employed to mitigate technical vulnerabilities or weaknesses.

Having said this, I feel OEVT could serve a useful purpose if carried out in partnership with voting system vendors and election administrators with the objective of identifying potential vulnerabilities and threats and developing a set of alternative technical and/or management guidelines for addressing such vulnerabilities and threats.

An essential step, as noted above, would be for prospective OEVT teams to spend time engaged, with local election officials, in the actual preparation for and conduct of an election. There is no substitute for this experience. The subtleties of the numerous potential threats and vulnerabilities that emerge during the months of election preparation as well as on election day cannot be anticipated or communicated by any "expert"

The concept of OEVT appears to arise out of an expectation or desire that the VVSG must produce voting systems in which nothing can go wrong with a certified voting system. This is both counterproductive and an impossible standard to meet. The EAC will never be able to issue a voting system certification under this expectation…a situation on which we appear to be bordering at present.

5. Would component testing (the ability to test and certify components as they are modified or added to an existing system) be beneficial to your jurisdiction[M1]?

Yes. Anything that can reduce the cost and speed up the process of modifying/upgrading voting systems would be extremely important. I used to be able to have my vendors fix things that were wrong, inefficient or just stupid about my voting system. That is no longer possible.

There are numerous modifications of voting systems that likely have no functional relationship to most other features of the overall system. Likewise, superficial changes should be identifiable and subjected to a less rigorous standard (perhaps an equivalency statement only) for certification than functional changes.

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?

Yes.

The VVSG should incorporate a section explaining what they mean and what they do **not** mean. What do the states need to understand about adoption or non-adoption of the VVSG and the implications for the their available voting systems. How can the states use the VVSG to avoid duplication of effort (ie., time and money).

Perhaps the VVSG should be limited to technical issues only involving system integrity and security. For instance, should the VVSG address the issue of voter privacy, which clearly involves matters outside the control of any set of hardware and software, or should it address only matters of data security within the system?

The only realistic purpose of the VVSG is to promote continual improvement in voting systems over the long run. Even aircraft safety standards are not expected to prevent all future plane crashes. Somehow the message has got to be understandably communicated to the users and evaluators of these voting systems….states, counties, voters, media….that the VVSG does not involve the pursuit of perfection ….only the pursuit of progress.

a. What needs to be added or removed from this document in order for it to meet what is needed from future voting systems?

As noted, few, if any local election officials have the time or expertise to read or understand the significance of the entire VVSG. I addressed specific issues in my comments and presume this is not a forum in which to to restate those in detail.

In general, standards need to be removed that are based on the assumption of uniform state procedure, eg., the “privacy” standards. Such standards, where state definitions and rules may exist, should be generalized to accommodate such state variations.

The VVSG’s reliance on manual auditing of paper records (under the guise of “software independence”) without any standards for judging the accuracy or security of such manual tabulation/auditing is contradictory to, and potentially undermines, the entire purpose of the VVSG.

Flexibility and a reduction in the cost of bringing new systems or features to market are essential if we are going to have “future voting systems” that are affordable by the majority of jurisdictions and that represent any significant improvement over what we have today.

b. How could the process of developing and vetting the VVSG be improved to ensure higher volume and higher quality input from election officials?

Start by having those writing the VVSG spend a 3-6 months working in local elections offices during the period leading up to and including a significant election.

Do not try to enlist major participation by election officials or vendors in new versions of the VVSG in presidential election years except on our turf.

Election Officials Roundtable
Friday, April 25th, 2008

Testimony of Russ Ragsdale

First of all, I would like to thank the EAC for the opportunity to participate in this roundtable discussion. I appreciate their efforts in gathering input from a wide spectrum.

Having served Colorado as the local election official representative to the EAC's Standards Board since its inception, I have been introduced to many of the paradoxes and mysteries posed by developing such a set of guidelines as the VVSG. Should systems be made so secure and accessible that their development costs put them beyond most jurisdictions ability to procure? Or should we, in the name of fiscal responsibility, cut corners when it comes to ensuring the integrity of our elections? Are the threats to election systems that some would like to see the VVSG eliminate plausible? Are election officials being intransigent in order to protect investments?

The role of the EAC is not an enviable one. They are routinely pressed into a position of compromise. And compromise may lead to a set of rules that ensure neither integrity nor affordability.

We, as election officials, owe it to the voters of this country to listen, learn, and offer input whenever the opportunity arises. The VVSG is not just setting forth a list of system specifications; it is potentially setting the course for how we conduct elections in this country for many years to come.

1. *The VVSG has more than one audience, including vendors and VSTLs. Do you consider county and state election officials as one of the stakeholders in the VVSG and therefore one of the intended audiences?*

a. If yes, is the document intelligible to you?

b. If not, how could it be improved?

Of course. Election officials will play a key role in shaping legislation that will determine how their state utilizes the VVSG. Election officials will be responsible for acquiring voting systems designed to VVSG standards. And election officials will be responsible for justifying the costs of these systems to their constituents and educating them in their use.

a. The VVSG is by its very nature a technical document. Its primary purpose is to convey to manufacturers what is needed from their systems for certification and to VSTLs what is required of the testing regimen; a document written by technically-oriented people, for technically-oriented people. At the same time, its impacts must be understood by election officials for the reasons previously stated.

b. I had the opportunity to testify before the EAC at an August, 2005 public hearing in Denver regarding the 2005 VVSG. I recommended to the Commission that they consider developing a "VVSG for Dummies" specifically for elections administrators. That recommendation still stands.

During the development of this iteration of the VVSG, NASED and both the EAC Standards and Advisory Boards have requested of NIST that it produce a plain language companion document. This document would be used by the "non-technical" community to better understand the nuances of the VVSG. In response to these requests, a draft of this companion document was delivered to members of the Standards Board in December, 2007.

This companion document focuses on material that is new or significantly changed from the 2005 VVSG and therefore requires, to a certain extent, a working knowledge of the 2005 VVSG. Due to a number of reasons, among them being that it was developed quite rapidly and no system has yet been certified to its standards, a minority of election officials possess this type of familiarity with the 2005 VVSG.

As of yet, this companion document is in draft form only and has had a very limited release. I would recommend that the EAC revitalize this effort.

2. *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.*
    a. *What are the essential elements of a risk assessment?*
    b. *How can the EAC best create a risk assessment that recognizes all possible risks and assesses the plausibility and nature of such risks in an election environment?*
    c. *How do you evaluate what is an allowable level of risk?*

a. I would not assume to be able to identify the elements of a risk assessment better than NIST could do. I would assume that they have been called upon to perform similar efforts or have the networking available to other agencies that have. With that said, one element that may be overlooked is the amount of resources or effort required to mitigate a specific threat. The use of a rating system, possibly as simple as a three-tier HIGH, MEDIUM, or LOW rating would be beneficial to help understand which threats require the most attention.

b. The EAC must first fully understand and articulate the purpose of such a risk assessment. If the purpose is to assist in developing testing specifications for the VVSG it may look much different than if it is to be used to create a "users manual" for elections officials. Many risk mitigations involve in part, or in whole, procedures rather than built-in system protections. An example of this would be secure storage of equipment. A risk assessment may conclude that continual video surveillance is necessary to secure stored voting equipment but how would that translate to a testable VVSG requirement?

At the December, 2007 Standards Board meeting, a resolution (2007-08) was passed asking the EAC to remove all requirements from the VVSG that mandate procedures rather than system standards.

While a more holistic risk analysis may provide useful information to the entire elections community, caution must be taken before including its findings in the VVSG.

c. After the risk is identified, characteristics of the risk are determined.

- Number of votes at risk. Is the threat likely to be a one-vote effort such as an individual casting a ballot at a vote center and attempting to vote again at another location? Or is it an effort aimed at a large number of votes such as introducing malicious code in the election management software?
- Determine plausibility and likelihood. Will it take collusion among several elections staff or simply the efforts of a single pollworker? Will it require defeating several levels of security (i.e., camera surveillance, userid/password, tamper evident seals) or a simple change of a log record? Will it affect the outcome of an election in a predictable manner or simply cause mischief?
- Amount of resources required to mitigate the risk. This is essentially a cost benefit analysis. If I dedicate an additional staff person for 6 months, I can prevent someone using concentrated ultraviolet rays erasing 1 out every 10,000 optical ballot scan marks….

If the number of votes at risk is few coupled with a very high investment and a very low plausibility, it is probably an acceptable risk.

3. *Could you comment on the value of stability in the standard to your jurisdiction?*
   a. *Which is preferred, a standard with a short-shelf life that accommodates innovation and change or a stable standard that may discourage innovation, but creates longer certification lives of voting systems?*

I would argue that a standard with a short-shelf life does not accommodate or promote innovation. Rapidly changing standards may very well stifle innovation by creating the perception of high risk; what is certifiable today is obsolete tomorrow. Rather, a well-constructed standard that focuses on performance not design will foster innovation more effectively. A “stable standard,” focused on performance rather than design should not discourage innovation.

4. *What is the value of the open-ended vulnerability testing (OEVT) model?*
   a. *Would the current OEVT requirement in the standard reduce or decrease voter confidence in your system?*
   b. *If the EAC were to require OEVT how could it best be included into the EAC’s Testing and Certification Program?*

As technology solutions develop rapidly, so do technology threats. OEVT allows systems to be tested against "new and improved" threats that may not be contemplated in established VVSG tests. OEVT also allows skilled teams to explore further any indication of hidden flaws discovered during routine testing. But OEVT is subjective and carries with it a potentially hefty price; cost of development which translates to cost of product, and a dampening of innovation.

a. OEVT often involves testing to failure, meaning that testing is not complete until the system fails. Regardless of the logic behind this approach and regardless of how well a system resists failure, the resulting perception will be that the system is vulnerable therefore decreasing voter confidence. On the other hand, if a system survives OEVT without failure, it may create a false sense of security that the system is flawless. This may result in increased voter confidence but wrongly achieved.

b. OEVT should be recommended and encouraged during system development. But to require it within a certification program is probably not appropriate. It may best be used to determine how well a system has matured, but not as a pass/fail test. How do other technology certification programs address OEVT? Voting systems cannot be the first technology to face this issue.

5. *Would component testing (the ability to test and certify components as they are modified or added to an existing system) be beneficial to your jurisdiction[M1]?*

Certainly. And conversely, prohibiting component testing, or requiring end-to-end system testing, will adversely affect my jurisdiction.

Testing a complete system end-to-end to the next VVSG standards promises to be a time consuming, costly endeavor. Requiring a complete system test when only limited component modifications are made will discourage manufacturers from making any enhancements to their systems until a complete overhaul is warranted. This will delay or eliminate incremental enhancements.

As an example; in Colorado, many counties are wishing to switch to a paper ballot, central count election method. Their current system manufacturer does not yet offer a high speed ballot scanner. However, the manufacturer did submit such a scanner for EAC testing in early 2007, along with an entire system, but has yet to receive certification. It is doubtful that this device will be ready for service by the November, 2008 election not because of any technical shortcomings but because of the length of the testing and certification process for an entire system.

If a manufacturer decides to proceed with a total system certification in order to add a component, the cost of testing will more than likely be applied to the purchase price of the component possibly putting it beyond reach of many jurisdictions.

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 in order for it to meet what is needed from future voting systems?

b. How could the process of developing and vetting the VVSG be improved to ensure higher volume and higher quality input from election officials?

As was discussed in the response to question 4, if or how OEVT is to be implemented needs to be carefully examined. It has the potential to increase development and testing costs significantly while not guaranteeing a better product.

a. As was mentioned in the response to question 2 b, the Standards Board requested that the EAC remove all requirements from the VVSG that affect election officials' procedures. However, I believe it is well established that the integrity of an election requires far more than any measures an election system alone can provide. Election officials must be included in the equation.

   This leaves me conflicted. The VVSG must be focused on the behavior of the system but at the same time, how the system is to be used must be considered. Requiring a system to be as secure as possible on its own without consideration of physical and procedural measures will result in complex, expensive products affordable by a minority of jurisdictions. This same can be said about accessibility. For example; rather than redesigning a DRE to allow for wheelchair approach, simply placing the DRE on a table without deploying the DRE legs results in the desired level of accessibility. And the table has a multitude of uses. An oversimplification indeed, but illustrative.

   In Colorado, systems that were recently recertified all had accompanying conditions for use. Through testing, a system's potential shortcomings were documented. But rather than discarding and replacing the systems at the cost of millions of taxpayer dollars, procedural solutions were arrived at through conversations with users and industry experts. While this process came under criticism from all angles, much due to its rather ad hoc appearance, it may have revealed a possible approach for the EAC.

   What happened in Colorado was done in retrospect, certifying systems that were already in place. The VVSG looks to future development and deployment. But nonetheless, identifying a system's shortcomings and, if not catastrophic, developing common sense procedural conditions may provide an acceptably secure system while not breaking the local jurisdiction's bank.

b. Election officials are by nature social animals. They are known to gather at annual events, sometimes even more frequently. If the EAC would develop a "road show" VVSG presentation, this could be used as both an educational and an input gathering tool. Most election official conferences would welcome EAC speakers and if EAC resources were thin, if the presentation was modularized, it could be delivered by specific state representatives from the EAC's Standards or Advisory Boards.