****

U.S. ELECTION ASSISTANCE COMMISSION

ROUNDTABLE DISCUSSION

DECEMBER 11, 2007

****

UNITED STATES ELECTION ASSISTANCE COMMISSION ROUNDTABLE DISCUSSION was taken before April C. Balcombe and Michelle Robertson, Certified Shorthand Reporters in and for the State of Texas, reported by computerized stenotype machine at the Omni Austin Hotel Downtown, 700 San Jacinto Boulevard, Austin, Texas 78701, on December 11, 2007 commencing at the hour of 1:00 p.m.

TEXAS CLOSED CAPTIONING
310 East 34th Street, Austin, Texas 78705
(512)480-0210

P R O C E E D I N G S

>> KING: Well, good afternoon everybody. We will get started here in just a moment. I think all the panelists are here. We have a few housekeeping items, if you would, the normal cell phones, Blackberries, anything that beeps, squawks, if you would either put it on silent or off would be appreciated.

The agenda for this afternoon is a panel discussion on five issues related to security in the draft version of the 2007 VVSG, and we have brought together a panel today of people with both experience and interest in security issues related to voting systems. And Matt, if you would, if you would flip to the next slide. Back up one. As I was preparing for my comments today, I was doing my normal Googling, looking for precedent. Always interested in historical perspectives on voting systems and technology in general, and I came across a

couple that I thought might help at least me get my perspective on this. And I think in fairness to Charles Dual, that is attributed to him, but I don't think he ever really said that.

In any event, Matt, if you would go to the agenda, this is an ambitious agenda. It is what we are going to attempt to hold to today. We have got five questions that we have been asked to address, and we are going try get a break into the middle. If we get fatigued we may break sooner, and we may break more often.

But what I would like to start with is asking the members of the panel to introduce themselves, and then we will have opening remarks from Brian Hancock from the E.A.C.

So Ron, if we can start with you and just work around the table.

>> I am Ron Rivest. I am on the computer science department at MIT.

>> I am Peter Ryan. I am a professor off computer science at New Castle University in

the UK.

>> My name Daniel Castro. I am a senior analyst with the Information Technology and Innovation Foundation.

>> I am Alec Yasinsac with SAIT Lab and computer science department at Florida State University.

>> Okay. Chris Thomas, Director of

Elections, state of Michigan. And Chair of the U.S. Election Assistance Commission Board of Advisors.

>> Sarah Johnson, Executive Director of Kentucky Board of Elections and the Chair of U.S. Election Systems Standards Board Executive Board.

>> Brian Hancock, I am Director of Testing and Certification for the U.S. Election Assistance Commission.

>> I am John Wack from the National Institute of Standards and Technology.

>> Good afternoon. My name is Costis

Toregas. I have two hats here. One is a computer science scientist in George Washington University, and I am also on the staff of Montgomery County, Maryland, advising the county council on information technology matters.

>> Michael Shamos. I am a professor in the School of Computer Science at Carnegie Mellon University, and I think I am here because I have done over 120 voting system exams for six states since 1980.

>> Hello, I am Juan Gilbert from Auburn

University, professor in computer science and software engineering.

>> I am Merle King. I am Executive Director of the Center for Election Systems at Kennesaw State University, and I will be moderating this panel discussion today.

If you look at the agenda, you will notice we have got five questions spread out over five hours and if you have figuring the overhead, we will spend 30 to 40 minutes per question. I am

hoping that everybody will kind of self-regulate themselves, and we will share the microphone appropriately.

When you do get ready to speak, if you would, either put your tent card up vertically or in some way get my attention, and we will try to move around the room as quickly as we can. But before we begin, I would like to ask Brian Hancock to give some introductory remarks.

>> HANCOCK: Thank you, Merle, appreciate it. And thank all of you for agreeing to participate with us here in this very important meeting. We know you have busy schedules, and we know that many of you have come from quite a

long distance in order to join us.

I should note that this is a first in a series of round table discussions that the E.A.C. intends to hold on the TDJC recommendations. We will have similar sessions with test labs, accessibility and usability

professionals, election officials, activists and manufacturers. Roundtable discussions will each continue to educate and inform the E.A.C. on specific areas of the document under consideration.

I also need to acknowledge Matt Masterson over there of the E.A.C. who did the majority of the work to make this roundtable discussion a reality. Matt is also the primary E.A.C. staff person available and working on a day-to-day basis dealing with next iteration of the VVSG. Before I turn the round table over to the capable hands of our moderator Merle King, I would say a few words about why we are here holding this discussion.

Beyond the obvious, that is to get input on the TGDC recommendations for the next iteration of the VVSG, I think we need to look at what we are trying to accomplish in a macro

sense. General goals of course are to develop an implement standards to make voting systems as reliable, secure, accurate, and accessible

as possible.

These rather simple words when spoken are rather simple words when spoken but as all of you know better than I do, extremely difficult to produce. By undertaking the development and adoption of a new iteration of the VVSG, the E.A.C. and its partners are charting the course for the development of voting systems in the United States for the foreseeable future. This is a truly awesome responsibility and one which we must undertake with full commitment and proper due diligence.

Given the scrutiny that this process specifically and the electoral process more generally is under, failure in this endeavor is certainly not an option. This is why we have invited you here today. The NIST and the TGDC work on these recommendations while extensive and very good is only the beginning of the process of development, review, and adoption. It is not the end. The real work for the E.A.C. election officials, academics, and the

American public begins now.

The questions we pose to the panelists as conversation starters related to fundamental aspects of the TGDC recommendations. The questions were asked so we can begin open and reason discussion on the direction we're charting for our voting future.

To open our round table, we ask the question related to the development of a detailed risk assessment framework for voting systems.

I personally feel that the development of risk assessment should be the cornerstone of framing our public debate about the VVSG. Others in the academic community agree with this assessment. Professor Douglas Jones of the University of Iowa has stated that, I quote, if we can quantify the costs of threats and defensive measures we'll be able to rank threats in order of their likelihood and defensive measures in order of their importance.

Professor Jones acknowledges this will be a difficult task but an essential task not only so we can judge the adequacy of our voting

system standards but also the adequacy of our recommendations for best practices and the adequacy of state laws and administrative procedures.

I thank you, once again, for joining us today and look forward to our discussions this afternoon.

>> KING: Thank you, Brian. If you can, Matt, move to the first question. I hope members of the panel as well as the audience can see the question as it is displayed.

But reflecting back on Brian's comments about the need for a risk assessment, I thought when I first looked at voting systems, that analogous comparisons were really inappropriate.

I would hear people say that voting systems should be like ATM machines or voting systems should be like lottery systems, and not only did I think that an analysis of those environments would not aluminate voting systems, I thought that may be harm done in the comparisons, because voting systems are

24 somewhat unique.

25 My opinion of that changed somewhat, in

1 part, based on presentation of a gentleman from
2 the Nevada Gaming Commissions IT Security
3 Group, and it opened my eyes that maybe some
4 other people are working with models that we
5 can learn from and would be appropriate.
6 So, the question about risk assessment --
7 and I am going to throw some items out for our
8 panel to kind of help form a starting point for
9 this discussion -- is some questions. And one
10 is: Have -- is there a consensus of the
11 definition of a scope of a voting system?
12 And for those of us who do systems
13 analysis, scoping the system is always
14 critical -- what is inside, what is outside of
15 the system.
16 Are there users? Are there managers? Who
17 are the stakeholders involved in the systems?
18 Have we defined the risk, and more importantly,
19 have we kept up with metrics by which to

measure risk?

Risk is the possibility of an event occurring that has a negative impact on an organization, so we think about risk in terms of the likelihood of occurrence and the impact of that risk.

Have we distinguished between inherent risks -- those are risks in a system for which there is no control -- and residual risk, risks that still remain once controlled are designed into a system?

Do our risk models presume a capability to audit all risk out of a system? And if you work with auditors or if you have done auditing work, we talk about the cost of auditing risk out of a system as you approach the 98, 99, 100 percent levels of certainty, the costs of auditing the risk approaches infinity.

And then another item that I really don't see talked about in risk assessment of voting systems, but we talk about it all the time in financial auditing, is the notion of reasonable

assurance. Do we have a metric? Is that in our lexicon voting systems of auditing to the point of reasonable assurance?

In auditing the credibility of the auditors in developing the risk assessment models are critical. In financial auditing, we see the auditors have credentials, they have experience sets, they have training, they have a code of ethics.

And the IIA, the Institute of Internal Auditors, one of the requirements to be an auditor is: Shall engage only in those services for which they have the necessary knowledge, skills, and experience. So even talking about who should be developing the risk assessment models can be a problem.

In looking at how do we assign weights to risk, how do we prioritize risks, in financial systems we look at are the risks associated with core functions within the organization? Are they associated with ancillary?

Are risks greater for -- for continuity plans; that is, contingency plans that enable an election center to keep functioning; or are the risks greater for disaster recovery plans?

The extent of the system, the change, are you looking at re-engineering the system or making trivial changes to the report generation functions of the system?

So there are many models in the financial world that enable auditors to identify risk, to develop models of risk, and very importantly, to reach consensus of those models for the stakeholders.

In the corporate model of risk assessment, particularly since the Sarbane Oxley legislation, the identification of who is accountable for risk assessment in the model, and then, finally, I think there was a question about what are the allowable levels of risk.

And I am a pilot, so I look at the NTSB reports frequently, and there have been six incidents at the Austin, Texas airport in the

past couple of years. And I got a ticket to fly out of there tomorrow, so I guess, by assumption, that is an allowable level of risk.

But we often don't talk in elections, we have a tendency to swing very quickly to the absolutes, and we don't talk about what is reasonable assurance, what is allowable risk.

So with what as my questions for the panelists to kind of open the discussion, I think Ron also had some remarks that he wanted to open with.

>> RIVEST: Thanks, Merle. I prepared some remarks that address both risk assessment and software independence. I think it is related.

I guess I should state first I am on the

TGDC, but my remarks today are my own. They don't reflect the TGDC in any formal sense of the E.A.C. or anybody else, so I am happy to answer questions based on my experience in the TGDC and so on.

The questions were raised, what are the risks in voting systems, how to assess them, what are acceptable and unacceptable risks.

And I think the best guide we have to that so far is the Brennan Center Report on the machinery of democracy. They did a careful study, looked at hundreds of different risks to a voting system, and tried to evaluate their severity.

They identified software is the most risky component in voting systems. The voting system may contain malicious code or code that is erroneous. It can change votes and cause an incorrect election outcome, perhaps undetectably.

Of course people are the source of most problems, and their metric, I thought, was a very interesting one, which is how many people are required to cause, say, an incorrect election outcome or a significant change in the

election outcome to happen.

So if you're looking at what are you

risking election, you're risking that we get some of the incorrect election outcome, if we don't get that right, then our democracy isn't working properly.

And another risk, an associated risk, is that the outcome is right but it is not believed. You don't have sufficient evidence to convince the loser or the populous or the voters that it is the correct outcome.

So the TGDC proposed this notion of software independence as a way of mitigating some of the risks associated with software. I want to talk a bit about it. It is perhaps the most significant aspect of the draft of the VVSG.

It is there to mitigate the risk of software problems causing incorrect election outcomes. So "software independence" means basically -- quoting here -- "that an undetected bug or error or malicious code in the software can cause an indetectable change in the election outcome."

Maybe it is more helpful to look at it the

other way around. Software independence means that you are placing your complete trust in the counting of the votes by the software or accepting any risk that there may be incorrect or even malicious software in the counting of the votes. So what is wrong with software independence? We heard lots of testimony in the TGDC that indicate software is correct and not susceptible to manipulation is beyond the state of the art.

This is obvious to people using the computers today. Gene Spafford wasn't able to make it here. He had some nice words that he put in his written testimony saying it really isn't possible to tell whether software or other technology contains what he called hidden functionality. So is it possible that this thing might do something sometimes that is not what you expect? That is just not part of what we know how to do.

And if you look at it from an actually how you would assess it, it is really hard. A voting system may contain 10,000 pages of code and any one page changing an I to a J somewhere may cause the program to misbehave at some

point which may not be revealed in testing but may happen in an election. This is particularly hard when the relevant software may not even be available to software systems. May depend on operating systems or drivers for which the source code is not even available for review by the tester. So it really is a tough problem. Be nice if it weren't so, but it really is hard.

So our voting systems certification will probably never mean that the software in the voting system is bug free and always gives the correct result. Guaranteed -- we just are not able to give that level of assurance these days. In addition, we have the problems of assuring that the software on the voting system is indeed the software that was tested in the first place.

California, I thought it was interesting, they have been top to bottom reviewed, revealed how easy it is on the existing voting system for a virus to propagate from one machine to

another, changing the software and every machine that the voting memory card went to.

So to mitigate these software independence

requires that the election outcome not be totally dependent on records produced by software. The voter must have the ability to directly verify his or her choices on a paper ballot, and these paper ballots must be usable as a check on the electronic counts, such as with a post election statistical audit. Any time you are trying mitigate risk, you fall into one of two major paradigms. You are either trying to prevent the problem, which is what you doing when you are trying to prove the software correct or detect the problem and recover from it and the paper ballots and the post election audit are really in that paradigm. Software independence fits in the detect and recover paradigm.

So the major concern is undetectable changes in the election outcome. You have got

to have a -- you don't want to be hood winked and not even know about it. I would like to view software dependence as very much like being a seat belt in a car. Cars may have undetected faults in the braking system or elsewhere causing you to end up in a ditch, and undesired outcome. Seatbelts prevent you from

the undesired outcome, you know, going through the windshield or whatever. Of course, you don't need to wear the seatbelts. You don't need to do a post election statistical audit but you should.

There is lots of issues with software independence, I mean, voters may not examine all their ballots. You need to consider that and realize that even if significant fraction of voters do look at their voter verified records that you do it in confidence that attempts by software to cheat the voters can be detected. And you realize there are advantageous when the voters actually read the ballots themselves in that regard. It is also

the case that a post election statistical audit itself may not look at all the ballots. It is after all, just a statistical sample. But it turns out to be, if you do the math, surprisingly cheap. I mean, if you have a five percent margin of victory, 20 percent recount will actually get you up to over to 90 percent confidence that you will have found fraud sufficient enough to change the election outcome.

Of course, an audit is not required by the draft of VVSG. It can't be since the draft VVSG is just about equipment testing and not about procedures. But a well-designed voting system based on the principle of software independence can yield election outcomes having a high degree of confidence that they are correct, that they correspond to what the voters' choices are. The risk of incorrect election outcome is mitigated by the use of these voter verified independent records and

the post election audits.

Back to the original question about acceptable and unacceptable levels of risk, I personally think it is unacceptable for a voting system to have the property of a undetected software bug or error or malicious code can undetectable change the election outcome. That is something we don't need to accept and shouldn't.

I also think it is unacceptable for any single person to change the electronic outcome, you know, even before the post election audit. And OVET can check for these kinds of things.

There are reasons for doing things like

the OVET that went into vulnerability testing that are outside of the integrity of the election. There are issues of voter privacy for example. Can someone figure out how you voted from the records created by the -- that you can't detect just by looking at paper ballots. You really need to look at the system and internal of that to tell whether voter

privacy is being well protected.

So there is lots of more to say about different kinds of risk. There is, you know, risk that we will miss out on new developments and technology and so on. We will be talking about that later. I think I have talked long enough.

>> KING: Thank you, Ron. With that, then I would like to open up the discussion to other panels and Mike.

>> SHAMOS: I think I would find it useful if we did a little more question defining before we got heavily into the topic. So how do you evaluate what is an allowable level of risk? That sounds like that it begs for numerical answer. That we are willing to accept one in thousand or one in million

elections going bad. And I am not sure that is what the question -- that is what the question really is. So I would like to start with a discussion of what we mean by an allowable

level of risk and how it would every be assessed.

>> KING: Okay. Do you have thoughts on that?

>> SHAMOS: Of course. I am not proposing an answer to the question. I can tell you about some experiences that we have had though. I was on the project serve review committee in 2004 for a system for internet voting for Americans overseas, and one of the exercises that we attempted to go through, which we ultimately discarded as foolish, was an attempt to place probabilities on various potential actions. So what is the chance that an intruder will try to effect the outcome of this election? I don't think it matters whether the chance is one percent or 100 percent. You want to prevent them from doing it.

If it is an issue that we are doing risk assessment so we can decide where to spend the money and spend a lot of money preventing the

risks that we think are very likely to occur

and then not spend very much money on the risks that we don't think that are likely to occur, that will increase the probability of the ones that we don't think are likely because once people figure out what we haven't protected, they will turn their attention to that.

And I think the whole exercise of risk modeling, the fundamental folly of it was brought home to me in the recent mortgage crisis. There was a company called Campbell and Company, which was an 11 billion-dollar hedge fund that lost 12 percent of its value in one day because of the failure of the mortgage market.

And when the CEO of Campbell was interviewed by the Wall Street Journal as to how this could possibly happen, his answer now often quoted, you can see many hits on the internet on this. He said, "Our risk models failed." And so you can develop the greatest model that you think you can develop, but if it is inaccurate for some reason, it is going to only give you false assurance that you have really guarded against something.

So instead of -- what I do favor is an exercise in risk assessment where you attempt to enumerate as many of the possible risks as you can, not necessarily signing probabilities to them. But then devise remediations for them and attempt to place a value or cost on making those remediations and then see what the whole picture is of weighing the necessity of evaluating intentions which is what you are doing assessing when you evaluate the probability of something occurring. So I didn't answer the question, but just to get things started.

>> TOREGAS: Two additional thoughts on the risk question. Do you, Mr. Moderator, encourage us to think about the scope that we feel comfortable with. And I think if I thought of the American voter, he or she is not so concerned about only the machines risk profile but the risk profile of the entire process of elections. And I know that the VVSG is looking at a machine, but perhaps we might think about how we could daisy chain risk models all the way up and down from end to end

25 of the entire voting process and the entire

1 election process so we could give that voter
2 the confidence not only in the machine but also
3 in the entire process.
4 The second concern that I have, and again
5 you mentioned it, that sometimes in a risk
6 analysis, we say 97 percent, we can fund
7 98 percent. We begin to run out of money,
8 99 percent, we are getting pretty close to
9 infinite and so on.
10 And the question therefore begs an issue
11 that we discussed in another forum about a week
12 ago, and that is the beginnings of some kind of
13 a cost benefit analysis which would help us
14 place the risk evaluation in the context of
15 components other than probabilities alone, and
16 you have mentioned one, which might be expense,
17 cost, how much are you willing to pay to
18 guarantee an extra nine on your string of nines
19 after the 99 gets done? And so those are the
20 two thoughts I wanted to propose that we spend
21 sometime on, cost benefit analysis, and the

notion that the scope of the risk assessment ultimately has to be an end-to-end process of the election process itself so therefore as we are looking into the VVSG at the machine

itself, how can we make it so that the risk model we discussed and the risk model someone is sent off to create can in fact be related to additional risk models up and down that chain. Thank you.

>> KING: John.

>> WACK: A bunch of points. Everybody said very interesting things.

One thing that I want to point out is that while a risk assessment, I think, is very well justified, very important, it shouldn't be used too much to arrive at decisions as to -- for example, you know, is software independence justified or not.

In my experience in this process, a number of people have said -- have come across with reasoning of the form of various things such as

software independence and whether we will have to continue to using paper records is going to be expensive, do the risks, do the threats, really justify this, prove it.

I want to point out, in the answers to these sorts of questions, there are a number of things that we have to keep in mind. One is that, as everybody knows, voting system is

complex information technology equipment.

And in fact, you can even argue in some ways, because it is used infrequently and when it is brought up, it has to run correctly, things of that sort. It might even be more complex than when we generally think of -- when we think of desktop systems in large organizations and complex networks.

There has already been a fair amount of risk assessment work in this particular area. Where I work in the government we have been in charge of writing guidance for other agencies on how they ought to manage their networks and manage their information technology.

And pretty much what is in the recommendations right now starts pretty much with the guidance that we have issued thus far. We have taken advantage of risk assessments in that particular area and have pretty much said, they apply to information technology, we think very much they apply to voting systems as well. So I would not like to see a risk assessment kind of start at the very beginnings and not make use of that existing work.

The other thing that I would like to say

is that, in an assessment of risks, I think it is important to not look solely at what sorts of threats are out there and the likelihood that they'll be exploited or what sorts of vulnerabilities, but also look at the usability of things.

One of the other things that has come across in doing risk assessments in helping to manage systems more securely is to look at their usability. Are they easy to manage? If

they aren't easy to manage, if the controls are difficult to use, they won't be used.

If paper records are produced that contain all of the information you need for very precise audits, but the paper is thin, it tears easily, it jams in inexpensive printers, it is less likely that audits will occur.

So the overall usability of the systems, the ease of managing them, the ease of using some of the audit capabilities that are out there today also have to be factored in, in this overall assessment, I think, to basically, ultimately arrive at what I believe the goal is, which is: Shall we go ahead with certain things that have been proposed, such as

software independence.

So maybe I am a little bit all over the place here in my comments, but I guess mainly what I want to say is, I think many things have to be looked at in this assessment overall, and I would like to just caution that we take advantage of what is out there already, in

terms of managing information technology, and also look very carefully at how well the controls that are out there today are being implemented and whether they are sufficiently usable.

Sometimes making things easier to use for people makes them far more secure than otherwise. That's really all I had to say.

>> KING: Okay. Alec?

>> YASINSAC: Yes, thanks.

Dr. Rivest mentioned the Brennan Center study, and that is an excellent study. In fact, there are a couple of excellent studies from there. And there are several sources, as John mentioned, of threat models out there. The California top to bottom review did an excellent threat model, and there have been several done at Berkeley and other places.

But from what I've seen, there has not really been anyone to try to put a structure on these things. The Brennan Center study is a

perfect example. It is a wonderful study, very comprehensive, but it is all rules of thumb, it's all expert opinion, and there is very little quantification laid down to it.

For example, there is no structure laid over those threats that would allow somebody to reason about classes of threats beyond the specific instance that Dr. Rivest gave of the ability of one or two -- a small number of people to have an impact. That was the exclusive focus of that particular study.

So how much impact a single line of code would have on the ability to conduct a safe election, there is really no way to reason about that with the models we have.

And so in order to even conduct an effective study -- and we have done it Florida state, now six of these studies -- and in order to conduct an effective study, you have to have a much more precise, much more systematic classification system to be able to detail what the threats are so that the threats can be

analyzed in the context of the system that is being evaluated, and those tools just aren't there right now.

>> KING: Thank you. I wanted to come back to something that Mike said about the mitigation of risks, and I am curious, from our two election officials that are on our panel -- because obviously, any deficiencies in risk mitigation cascade down and accumulate at the implementation level.

I am curious whether you have any thought on the role of risk mitigation at the implementation level, as opposed to higher up in the development cycle and the design. I don't want to put you on the spot, but --

>> JOHNSON: I think it is extremely important to have it at that level, too. I guess we're sort of -- like the individuals have already said, a cost benefit analysis is something that is very important to us, because we obviously have to, you know, afford to purchase them and keep them up, and also what John is saying the usability and trying to marry those two, keeping all of that in mind, when you're developing models, the assessments,

and the classification system is very important to us, as election officials, because we have to take that system and obviously go back to our local, county individuals and then our, you know, precinct officers, who are predominately elderly, to be able to use these machines, much less the voter.

We see the forest, and it is a pretty big, thick, dense forest right now.

>> THOMAS: I would concur with Sarah. What we have up there are methods of avoiding risk that come from older systems, and we're now bringing new systems in, so there is this process of trying to adapt the older checks and balancing and the other assessments.

The higher up that is done, I think that is a good approach, but when it ultimately comes down to the implementation, which is with all of these folks -- but that's the next level that is really going to integrate these new systems into what our current laws, procedures, and whatnot have to avoid the risks.

>> KING: Alec, I wonder if you have a

24 comment on that, because I think Chris has just
25 added another dimension to your observation;

1 and that is, the legacy threat models may no
2 longer be appropriate to the new technologies
3 that we're rolling at.
4 >> YASINSAC: Well, I think that is
5 absolutely true. It really boils down to the
6 notion that led to software independence, is
7 that changing -- electronic changes can be
8 very, very easy in large scale. Changing paper
9 things in large scale generally is very, very
10 hard.
11 Conversely, I am not sure that the models
12 for protecting paper have moved forward to
13 match the precision that is now demanded in our
14 elections and the ability to report quickly and
15 report accurately and the conflict that is
16 created between the reporting of the first
17 count as an electronic count that may not
18 include all of the ballots, that may not have
19 the precise construction of all of the input of
20 the public, and then producing a second count

that has additional information that may
conflict with the first count.
So just the damage to public confidence
that that notion has is something that, I
think, hasn't been addressed, and it is

directly because of the emergence of the
electronic aspect of voting.
>> KING: Yes?
>> TOREGUS: Just to piggyback on that, on
Section 8 of the VVSG, there is a beautiful
diagram, a process diagram, of what happens
during an election, and stimulated by what
Christopher -- if I might call you that --
mentioned. I wonder if the people who put
together that flowchart were able to somehow
put it side by side with what people might call
the legacy process and make sure that the kinds
of computer relationships and the computer
standards that are now being promulgated are
being based on a theoretical concept or on a
concept that actually matches the reality on

the ground.

I am not speaking about whether the reality on the ground is good or not. I am just saying that if it is not matching, then we're going to incur significant change management cause of every organization that conducts elections.

And whereas we can easily -- let's say that -- easily change something that the

machine does, when we talk about thousands and thousands of institutions, we have to be a little bit more cautious.

So to look back to my question, when the -- I think it was 8.1.2, when the procedure diagram was put together, was that an idealized procedure, or does that reflect the current state of practice in the field? I would like to know that.

>> KING: Okay. I think we're going to find out.

John?

>> WACK: I don't know if you will not.

First of all, thank you for calling it "beautiful," "pretty," I don't remember, but if you like them, I have some artwork myself that I could interest you in.

The models were put together by researchers at NIST working with members of the TGDC, but also looking at previous models, diagrams and talking with numerous election officials who have been involved in the development of previous versions, and they simply form what is thought of as kind of the general flow of operations, general flow of

what happens in various aspects of voting, pre-election and so on, so forth.

And it is there sort of as a framework for the requirements. In other words, you know, the requirements are based upon the general practice, you know, as shown by these flow diagrams.

Are they up to date with existing practices? We believe they are. But I should

caution that they are also fairly general. They don't get into too many specifics. They're intended to be kind of what you would normally expect to happen, regardless of what state or what county.

And then I also wanted to piggyback myself on Alec's point, too, about just emphasizing again, that, for example, if software independence results in -- well, the VVSG, or the recommendations, I should call them -- refer to it as an independent verifiable record, but if it is pushing paper, that's fine and dandy, but an assessment of all of this needs to ensure that paper itself is sufficiently usable to be used as an auditing tool.

I think that that may have got lost a little bit or maybe not addressed as well as perhaps it needs to be. We've heard a lot of feedback from people in the election community.

And essentially if it's -- if an approach like this gets used generally, it has to be

extremely usable, and more work definitely could be done in that area.

>> KING: Okay. Juan?

>> GILBERT: Yes, Alec's comments prompted me along a certain line of thinking. I am not a risk assessment expert, but it brought up some questions when you mentioned the Brennan study and some studies you have done.

One of the things, when we're talking about software independence, is there such a thing as risk assessment independent, such a way that the risk is independent of the specific voting equipment?

So listening to the conversations we've had so far, it appears that -- it sounds as if the actual assessments are highly dependent on the actual equipment that is being used.

So one of the things that came to my mind is this idea of classifying these threats with

a different metric.

So I had a question for you, Alec. Is

there a metric such as the number of ballots impacted by a threat to be used to classify threats? So if you had a metric such as that, to me it appears that would be independent of any system.

So if you had catastrophic, moderate, low, none classifications, and you had a number of ballots that were impacted by each level, if you had such a model, would that be independent of any system? That's my question. And does such a model exist? That is my question.

>> YASINSAC: As I said, I am not aware of one that exists, and I did put one together for this panel, but I didn't get it in time to be distributed.

And one of the attributes of the model that I constructed was the impact, and I did not go so extensive as you, but exclusively mentioned that it was wholesale or retail. Either it was a large-scale attack or a small-scale attack of a few ballots.

So that is an attribute that I think is essential to a threat model. And there are a

number of them, as I have been working on this, actually, for a good period of time, and interacting with a lot of different people, there were many attributes that popped out as being obvious to me that they fit in.

Where that kind of model obviously gets difficult is when you get further down the tree and you need to know what level of detail is appropriate to not exclude some equipment or some types of systems, and then to take the discussion pertinent to the threats on the scale that you need to be able to discuss, whether that scale is for cost, for risk voidance at the point of the elections officials, or for consideration of developing new and innovative solutions for voting systems, how do you design that threat model.

So it has to be -- but I think there are a group of attributes that are widely acceptable and that we could identify if we were to spend some time on it.

>> KING: Okay. I wanted to add, too, I had the opportunity to see a presentation by the state election director of Louisiana on their contingency planning model, and that's an

interesting model to look at in terms of realistic assessment of what can go wrong in an election in a scale that is really staggering.

So perhaps in addition to the models that have been discussed, there are some things that are in circulation out there already that can be brought in.

What I would like to do, if there are no more comments on this -- I am sorry. Peter?

>> RYAN: Yes, I would like to follow up on Brian's comments about the measures, because we actually toyed with a very similar sort of measure back in Utah that was slightly a different measure of impact on the number of votes that can be changed divided by the number of people who would have to collude in order to do that.

That seems to be an actual measure in some respects. It seems to work quite well in a class of systems, but we quickly realized if you try to push it to the extreme, it starts to break up.

The classic example is, if you start this, to think about the graphic schemes. There, the idea is to achieve software independence and so

on. Perhaps the risk boils down to, is there some undetected flaw in the mathematical arguments, the logic, and crypto, and so on and so forth.

So there you get experts that look in the system and judge [Indiscernible] and so then, the number of people who, in some sense, might collude in making a mistake of the system, is an entirely different kind of class of people than the class of people who might work with election officials.

So you try to -- I usually try to apply this measure across the entire spectrum of system, and I don't think it works for that kind of reasoning.

For example, if you are ignoring it -- the kind of person who would be involved, I hardly think that Ron would find a flaw in the system and keep it to himself or something. The odds

of that happening are astronomically lower than the a number of election officials at a polling station colluding to undermine the outcome of a polling station. So these kind of measures are interesting, but certainly, if you want go across the entire spectrum the system, I guess

it gets a bit dodgy.

>> RIVEST: I think the Brennan Center, some aspects, I think they were talking about election officials would certainly be expected much higher integrity than a typical voter, you know, where if you are doing something like chain voting where you just have to persuade a voter to turn over their vote, that would be persuading an election official to violate their oath, so that would be a much, much higher barrier. And so I think that that kind of consideration is very relevant, yeah.

>> KING: Yes, Costis.

>> TOREGAS: One last thing on 1B or 1A, you asked how do you value what is an allowable

level of risk? It seems to me that we also have to stop and pause and think who says allowable? And ultimately, from my experience of decades of working with government officials, ultimately the people that have to decide what is an allowable level of risk are not the so-called experts, computer scientists or even the industry, but it is the people who are actually going to buy the machines and make sure that elections run well.

So we have to start thinking about how do we communicate very complex issues of risk assessment and risk management to people who on a daily basis have to make very complex decisions? Somewhere along this line we have to start thinking about communication to other sectors. And that is something that I am very much an advocate of, instead of having sectoral dialogues like we have a computer scientist and then the advocate groups, I think we have to learn to begin to discuss things across those groups because without doing that, it is very

difficult to identify questions that I have just raised such as who defines.

>> KING: Costis, do you think that is also related to something I think we have heard from two panelist about the need for an expanded lexicon and a taxonomy so that we can -- when we do share these ideas, it is an accurate sharing of the ideas? Okay. Mike.

>> SHAMOS: In response to the question of who defines, initially it is the state legislatures. And typically when they have acted to define the allowable level of risk, they have defined it as zero. There are

numerous requirements in statutes in all the states that refer to things like absolute accuracy and prevent every person from interfering or tampering with the equipment. So they are phrased in absolutes.

For federal -- elections for federal offices, it would be the Congress. There is already a definition of an acceptable error

rate, and it will end up being left to the VVSG to say what an allowable level of risk is because the states will inevitably accept that unless so it is out of kilter with their expectation or what is publicly acceptable.

If you go up to somebody in the street and you say, what is an allowable level of risk that somebody could steal an election? They would say zero. We just can't have it. That is completely unrealistic of them to say that. But it is certainly the desire.

We have had a lot of useful discussion about this question. Unfortunately, I have the feeling that we didn't answer it. So I am not sure that what we have done is of great utility to the E.A.C.

>> KING: If you would and I have

another -- I have several here on the table. Mike, I think that is going to be recurring dilemma throughout today. But what the E.A.C. has asked of us and the Standards Board is do the best that we can, and I think along Costis'

suggestion is get that dialogue going. And I did not see the order in which things went up here, but Chris I saw yours first, so I call on you.

>> THOMAS: Just a quick comment. Addressing what the E.A.C. can do. And one, I would give the E.A.C. credit and Brian Hancock in particular for his Denver conference that he had earlier this year that did exactly that. Bringing together the various elements.

And the other thing I would point out is that the E.A.C. is moving forward with management guidelines. And to some extent, management guidelines are analyzing risk. In other words, how really you modify the legacy system and how you operate elections with these new systems.

And this comes back to beg the question, who makes the risk analysis? And obviously it is not any one sector. It needs everybody to

be involved in that. And as Michael indicated,

ultimately legislatures are the ones that weigh in there, and I think they would find some decent guidance coming from a federal level with input from the wider community and making this risk analysis. As opposed to just them making the analysis, which as Michael indicated, they are rarely going to do anything more than zero.

>> KING: Okay. Thank you. Daniel.

>> CASTRO: In response to, you know, question that we have been talking about about what is an allowable level of risk. I would argue that one thing is that is what states and Congress is willing to pay for. I think when you ask the people on the street, yes, they want zero and legislators want zero risk. But as a public policy question, this comes down to how much are you willing to spend? And this is what Costis was talking about.

I do want to go back to another point that we have talking about in terms of risk analysis, and it seems like there are some consensus at least that we -- there is no defender of risk analysis that has been done

yet and more work here.

When you are doing a risk analysis, there is a number of steps but among those you have prioritizing risk, identifying policies to respond to those risks and then choosing the best implementation for those policies by doing a cost benefit analysis.

It seems like, and I don't want to get ahead of where the discussion is going, but if we are saying that software independence is the policy we want to choose, it seems like that is getting ahead of ourselves because we haven't completed the risk analysis yet and we haven't completed the cost benefit analysis to decide if that is the policy that we should accept.

>> KING: Okay. Thank you. Ron.

>> RIVEST: Yeah, I wanted to respond to a suggestion that Mike Shamos just made that the VVSG may be the place where the allowable level of risk is determined. And then in some sense, you know, what the VVSG does is sort of set up the proposal or maybe not VVSG, would set up a framework of what can be certified. But the actual risk that is run by any election jurisdiction, really depends on the procedures

as much as anything. What it does is provides a range of acceptable levels of risk.

The question really is, does the equipment that would be certified support, you know, a level of risk controlling the risk in a way that would satisfy the potential customers, the election officials and the voting public? You know, for example, I mean you may have election equipment which, you know, provides the option for chain voting, for the voter, if they can take the ballot outside the polling place and exchange it, that is a say procedural question.

Similarly, there may be an option on the voting equipment which allows for a set up validation so you can check the software on the system is really the software that is supposed to be there. But those are procedural choices that the jurisdiction has to find as to how to enforce voter movement or either to exercise -- the question in some sense is does the VVSG, you know, provide a range of choices to the

22 election officials that allow them to get
23 within their comfort zone for a level risk.
24 >> KING: Well, thank you. I think that
25 is an excellent start in terms of the scope and

1 the level of participation that we are looking
2 for in these questions. And in order to keep
3 on the schedule, I would like to remind the
4 panel at the end of today, towards five
5 o'clock, there is going to be an opportunity to
6 each panel member to come back and address
7 issues that either have become better formed in
8 their mind during the panel discussion or that
9 they really want to make sure or emphasize, and
10 I am trying to also take notes to help with
11 some summation of those points as a way of
12 prompting our memories when we get to that
13 point in it.
14 But at this time, I would like to move to
15 the second question. Matt, if we could. The
16 2005 VVSG states one of the goals for the next
17 iteration of the VVSG was to create performance
18 standards that promote innovation rather than

19 design-oriented standards that limit design
20 choices for potential manufacturers.
21 And Juan, I think you have agreed to open
22 up the discussion on that topic.
23 >> GILBERT: As you can see, there are two
24 direct questions underneath that initial
25 introduction and getting right to those

1 questions, you know, where does this document
2 meet or exceed this goal? Where does the
3 document fall short? When I read the VVSG, I
4 think what I liked about it very much was the
5 performance standards are clearly defined with
6 respect to, for example, evaluation, actual
7 metric that need to be measured and calculated
8 and the associated benchmarks.
9 Now, I think these are things that are
10 good for the VVSG or any standards guidelines
11 to specify these kinds of things. So I applaud
12 the VVSG for putting those in there. Now, I
13 know some people will question the values for
14 those benchmarks and say, are those valid and

how broadly can they be generalized? And I have a comment on that in a second.

As I address the second question up there, is the concept of software independence as defined by the TGDC recommendations too technologically restrictive? If so how would you change it to be more expansive to include more innovation? So these are two questions we will address.

Now, I think the language in the VVSG is clear on software independence. In fact, I

could take it and give it to a nonsoftware person and say, here, read these two sentences that define software independence and they say, oh, okay, I got it. To me, that is a test to say the language is clear. And so that is, I think that is an accomplishment in the VVSG.

Now, although I consider this to be an excellent start with clear language, the VVSG also says that it makes a statement that paper schemes are software independent as an example. And I think there are issues and questions

about making such a claim, does that exclude other things or is that a strong recommendation to use paper? Which brings on my next point, which is, getting to innovation. Looking at the VVSG in my opinion, I think functional requirements versus hardware and software requirements are pinnacle and most important.

And I think the VVSG has these functional requirements in there. I think that promotes innovation. There is going to be debate about the different benchmarks and metrics to say how did we come to those and do those across? But I think the definition in particular for the innovation class gives you the opportunity to

challenge some of those if you do have innovation.

After a few innovations are considered, I think we will discover how well VVSG accommodates those. But I don't think we can get into this mode of what I call analysis paralysis, where we overanalyze something to

the extent where we never get anywhere and never even get a case to test the VVSG.

So what I like to do is cut my comment short. I could go on with some additional things, but I would like to get into answering those questions up there, the two bullet points. And I think that is a good way to lead the discussion. I turn it back to Merle.

>> KING: Thank you, Juan. Daniel.

>> CASTRO: Yeah, I just wanted to start off by -- I mean, the question up here is I think a good question. And it goes to the point should we have functional standards or design standards? But just starting off and I will put this out there. I would guess there might be some disagreement on it.

I do think the software independence although it is -- I say this in my written

statements, it uses functional standard language but ultimately it is really a design standard. When you look at it, the end result of it is it is forcing voting systems to only

use software independent or any voting system that is not using software. To me, that is a design standard. So when we are looking at this, yes, I would say that is technologically too restrictive. Whether or not that is good or bad for security, we can discuss that. But is it a design standard or functional standard? I would say it is definitely a design standard.

>> KING: Okay. Thank you. Mike.

>> SHAMOS: So I think there is a significant block of folks on the panel today who have issues with software independence as a concept. I am one of them. And what I want to do is raise the what I think are from my point of view the major issues. I think software independence is unarguably wonderful, warm, and maternal. We certainly don't want to say that it is okay for software on its own to influence the outcome of an election. And I don't think though that by rejecting software independence we are saying that it is okay for software to

do that.

So it starts out with a kind of -- with a motherhood feel to it that seems hard to argue against. It doesn't go far enough. What software independence says is that the software itself can cause an undetected change in the outcome of an election, but it doesn't take into consideration other things that might cause an undetected change in the outcome of the election.

What software independence says is you can't rely only on the software. You are going to rely on something else. And yet there is no discussion of the something else and its integrity, and if the something else is handling of traditional pieces of paper in the traditional way that have always been used to influence the outcome of American elections, then software independence isn't so good. Because what it is doing is turning over the responsibility to system that have known flaws, and so I think software independence, if there were another statement that said what is the other thing that we are going to rely on if we are not going to rely on the software, and we

could evaluate that, then we would get somewhere.

There has never been a comparative study of the security of D.R.E. systems with the security of paper-based systems. It has never been done. And there seems to be a belief that once you put something on paper, it either becomes sacrosanct, is unalterable, or over the centuries we have developed these excellent paper handling methods that guarantee that no human being can influence the outcome of an election.

How about if we had a standard of human independence, which is so to say that no undetected human can cause an undetected change in the outcome of the election. You wouldn't argue that either. That is a motherhood kind of thing to say. We know probably can't achieve that either. And I think that what we are doing by requiring software independence is frankly I think it is a subrose way of simply mandating paper trails.

Because the VVSG itself even says that the only known systems that achieve software

25 independence are paper trail systems, and it

1 admits begrudgingly that possibly somebody
2 might come up with something else in the future
3 but they are relegated to the innovation class
4 for which we have no standards because we have
5 never seen such a thing before because we don't
6 think it can be done. And I think the effect
7 that has on potential developers of software
8 systems is extremely negative.
9 Also, I haven't been able to find another
10 field of endeavor, maybe somebody can enlighten
11 me in which software independence is a
12 requirement. Not in the handling of nuclear
13 weapons, not in the handling of passenger
14 airliners that's hold 750 people. Not in the
15 handling of trains and other devices in which
16 human life is at risk. We don't require it
17 there. And the reason is we don't know how to
18 make software independent systems. There is no
19 book. There is no manual. There is no set of
20 standards that tell you how do you make a

system that is completely software independent.

What are the other things that you are going to shove the responsible on and how do you make those good? And so to show up with a set of standards that say, ahh, we have this

magic thing called software independence and you have got to have it. We can't tell you how to do it, but you have got to have that. And oh, by the way, pieces of paper do it. That is not hanging together for me.

>> KING: Alec.

>> YASINSAC: Stole a bunch Of my comments.

>> SHAMOS: I am sorry. I should have let you put yours up first.

>> YASINSAC: I think there is no doubt and in fact, I think most of the folks that propose software independence would agree that the goal here -- and in fact it was in Dr. Biford's statement that he just doesn't feel like a voting system can be devised that doesn't have a paper trail. And I think that

is a fairly common opinion among a lot of the folks, in fact maybe everybody universally that supports the software independence viewpoint. And it is understandable.

I certainly understand why it makes a difference, as I mentioned before. It is clearly harder to change lots and lots and lots of paper ballots in a single stroke of the pen

or single movement of the keyboard or to generate. We can argue the merits of that at length and ad nauseam. But what I would like to suggest and ask is part of the VVSG and a part of the consideration of moving forward, instead of arguing about whether it is a paper trail or an amendment or not, is to back up and try to describe what the properties are that we want this paper ballot to have.

Does it have to be human readable? Does it have to be immutable and in what sense does it have to be immutable? Does it have to be storable? Does it have to withstand heat?

Does it have to be something that can be seen or something that can be read or interpreted in the disabled community without any help or without devices? What is it about this paper trail that makes it essential to the voting process?

Because none of that that I can -- I couldn't find any of that in the VVSG myself. There was a discussion, I believe, in chapter four. But the definitions for example of IVVR and VVPT and VVR in the document were really circular and were of little to no help. The

discussion of the testing gave a better insight to the notion that software independence requires something that people can see. Something that they can feel. What are the driving properties of that medium?

>> KING: Okay. Thank you. John, I think you were next.

>> WACK: Let's see. My role is with regard to this question really is just to talk about what is in the VVSG, and I wanted to

point out that I think the TGDC has the resolution for software independence in December of 2006.

And so the immediate question after that was let's make sure that those systems that use paper records do so in a way that is as usable as possible or as usable as it is possible to make them in the amount of time we had available. So the requirements for example for voter verified paper trail systems were in my opinion improved a good bit, especially in the way that paper is dealt with. The reliability requirements were approved a great deal to ensure that failure rates of printers and accordian jams of paper and things of that sort

should not happen.

And then ultimately in the testing, there is a large scale volume testing approach. Where in essence there is going to be a mock election as part of the testing campaign. And systems will be tested pretty much from the

beginning to the end and end testing. And that in itself, in my opinion will put to rest many problems with voting systems and many problems with use of paper records.

So I do believe that while S.I. states a goal, that it is backed up with more attention paid to making sure that paper records are usable. Could more work be done in that area? Definitely so. I think that is definitely true. Could IVVR be examined more closely and more of a performance aspect be given to the requirements. That is definitely true. I think though that what is in there essentially constitutes good starts in those areas. And I would like to just make sure that people look at the area first and form conclusions afterward.

>> KING: John, if can I ask a follow-up question, and then I will go to Peter and Ron.

In one of the projects that preceded the NIST management of the VVSG was the IEEE P1583 project. And on that project, we struggled

with the notion of functional specifications versus design specifications, curious if those kind of questions came up early in the NIST project and how those were resolved.

>> WACK: Well, they did, and they are terms of art to a certain extent, and the conclusions I, myself, drew and some others were that you could go down a rathole pretty quickly arguing about what is a design requirement, a functional requirement, what is a performance requirement.

And design requirements, for example, which supposedly limit the design to a specific approach, are not necessarily bad. Performance requirements are not necessarily good. Performance requirements, where they make sense, are good.

For example, in the VVSG, there are performance requirements for usability of interfaces, and the performance aspect really is: We don't care what it looks like, to a large extent. We don't care how big it is, how

small it is, what color it is. We just want to make sure people vote accurately when they use it. So you're writing to a certain performance level of accuracy.

In some other areas, security is a good example. It is not a good idea to strictly say, it must be secure. You know, you have to get -- well, it is probably a complicated discussion, but there are a number of ways in which security controls can be implemented incorrectly, and so to a certain extent, there has to be some fairly specific design-related requirements.

I would say, though, in general, we wanted to go more towards performance-based requirements, obviously because it just makes it easier for vendors to come up with good solutions.

So I think that was pretty much what people wanted to do. In areas where that didn't occur, perhaps that can be approved upon in the second draft. But in some areas, I think it was justifiable to stick with design requirements.

I did mention functional requirements.

Functional requirements are how a system -- what a system ought do, and they're kind of in-between design and performance. And again, I'll reiterate, you go down a rathole pretty quickly with a lot of these terms.

But in general, yes, we wanted to go towards performance as much as possible.

>> KING: Thank you, John.

Peter?

>> RYAN: Yes. Well, there is quite a few issues here which need clarification. I can't speak to the details on how things are worded in the document. I can speak from my own point of view.

To me, certainly software independence doesn't mean paper audit trail, certainly, in the sense of a VVPAT, human readable, necessarily. That is the first comment I need to make. If that's what the document seems to imply, that would be an unfortunate phrasing of the document.

The other point is that, certainly when I came across the term first, I guess from Ron, I

took it as meaning it is not the be end, the
end all.

To answer Mike's comment, yes, I fully agree if you make the system, it's dependability is independent of the software, but you need to also investigate a lot of other things. And to a lot of us, myself included, one of the goals we're going through is to make the particular integrity of the system independent of essentially all components of the system -- including human beings, hardware, and so on and so forth.

So I viewed software independence as a sort of first step, I guess largely on the grounds -- as I think Ron pointed out -- is to make sure it is the most critical, most vulnerable piece of system, for example, D.R.E. systems.

So that was my view, that was the first step, but surely, we need to go beyond that. And my final point, I think, is that you can go

beyond that.

And there seem to be certain comments here that systems don't exist or seem unconceivable that could achieve these goals of software independence and perhaps independence of humans and officials and so forth.

And I think we have a group of concepts, several of us, that say that is actually not true. Now is not the time to talk in detail about them. But I believe such systems do exist, at least in theory.

My question is about whether if, in practice, they're pretty reliable and we have to argue about the cost of employing them, and whether they are credible in the eyes of the electorate at large, the stakeholders, and issues like that.

But in principle, I think there are systems. We have a group of concepts that something like this can exist. I'll leave it at that.

>> KING: Ron?

>> RIVEST: Thanks. I also wanted to respond to some of the points that Mike Shamos raised with respect to software independence.

You brought the airplane analogy, which is one that is commonly brought up, and I think it is an interesting one to sort through and to think about.

It is actually an interesting one for lots of reasons. An airplane is actually the prime

example of multiple redundant systems and backup systems, which is really what we're talking about with software independence here, is having another way of being able to achieve a vote count.

They've got multiple hydraulic systems. If one of them goes down, you have another one there. The pilot has a separate oxygen tank and oxygen mask, in case there should be decompression, you know, so that he can fly the plane even in spite the failure of a compression system.

There is even talk about the plane being able to land itself if it should be overcome by a terrorist and such. So there is lots of mechanisms for protecting against failure of any one given component.

But even more so, the airplane analogy doesn't go far enough because, when you think about it hard, voting systems have a higher calling, if you will, than an airplane does. An airplane, when it functions correctly, gets the passengers from point A to point B. When you are there, you know you're there, and you know you're in the right town. Although when I

landed in Austin last night, the taxi driver said, Do you know where you are? I said, No. He said, You are in London. This is London, England weather. But you know where you are when you get to the airport.

So the correctness of the operation of an airplane is sort of self-evident when you land at the airport. The correctness of the voting system is not so self-evident.

A winner is announced, and you wonder, is that really the correct winner. It is not as obvious as being at the airport in Austin, Texas.

So I think a voting system has to meet a higher calling. It has to be not only correct, but demonstrably correct. You have to be able to demonstrate to everyone, the voters and the losers, that you got the right answer, in a way that, merely pointing at the software and saying, this software is certified and we think the software in the machines is the same software that is certified and there has been no viruses, etcetera, probably does not suffice for a lot of people.

So the difference between being correct

and demonstrably correct I think is part of the point. It certainly is possible and maybe not even hard to write D.R.E.'s that are correct. I think we realized that early on in the work at the TGDC.

The hard part with the voting system that is all software is to make the results demonstrably correct. How do you persuade somebody that it is actually giving you the right answers? And that is a near impossible task.

>> KING: Thank you, Ron.

Juan, you next, and then back to Mike.

I was struck by something you said, Ron, about voting systems having a higher calling, and I think all of us in the room agree to that, but I am not sure where the charter is for that.

Because we talked earlier today about, in risk assessment, that normally is something that is done off of a collection of priorities established by the organization, and I don't disagree with what you said.

But as we start to look back for the artifacts that prove that or attest to that,

that could be very helpful in establishing some of our risk models.

Juan?

>> GILBERT: I think the gentleman --

>> KING: The gentleman from Auburn is --

>> SHAMOS: Yes, he wants the last word.

So as far as airplanes, yes, I agree, that the analogy is certainly not perfect.

But I was struck by something you said, which I liked, and I am going to throw it back to you to confirm that you really said it, which is that redundant systems on the airplane are sufficient.

If that is true, then if we had redundant software systems in a voting machine and the two were really independent of one another, they were different code bases, came from different places, etcetera, it seems to me that ought to be able to satisfy the requirement of software independence; that is, this other thing that we're talking about, that is going to take the reliance on software A could be software B. I don't think you're going to say yes to that.

>> RIVEST: Can I answer that, please?

>> KING: If it is a short answer.

>> RIVEST: It is not a short answer.

>> KING: Answer, anyway.

>> RIVEST: So the -- that's a path which the TGDC explored at length. I mean, you're following down the footsteps of thinking that the TGDC went when it was involving the VVSG.

It seemed very attractive at first, to take that analogy of redundant systems in looking at redundant software systems to try to provide that confidence that you want.

In the end, there are no marketplace examples of that, first of all. And in the end, it seemed that that was actually an illusion. You were chasing after a mirage most likely.

It may turn out to be workable in the end, but I don't think it is likely to happen real soon for the following reason: Because independence is an illusion, I think, when you try to build such a system.

How do you build such a system? You have vendor A producing part A. Vendor B producing part B. The election officials need to choose it. Well, they need to choose some system

integrator to put those parts together. The system integrator is looking for the code of part A and part B. The independence is lost at the point you're putting it together.

And so I think the idea that you can actually combine disparate systems in a way that preserves what you want. The independence, is extremely tough to do in practice, because you would have middlemen stepping in right away to provide lack of independence, to provide a single point of accountability for the election officials should something go wrong, and then they will be able to play with either system and change the outcome.

Second of all, you have the issue of being demonstrably correct as well, which you still have two software systems which are complicated, and then trying to argue that they're both correct.

It is very common with inversion programming to see programmers making the same

errors. It happens all the time when people do studies. So it is not any way a guarantee that you're getting the independence you want.

And finally, to answer the question, where does the charter come from for demonstrably correct, I think the legitimacy of the government, the elected officials, the voters want to see depends on the confidence of the election. That is where the charter comes from, is being able to demonstrate in a convincing way to the voters and to the losers that the outcome is correct.

>> SHAMOS: Okay. Thank you. I had yielded temporarily. I want to finish up my comments now.

>> KING: Go ahead, Mike.

>> SHAMOS: I don't know if it would be a surprise to anybody or not, but there is no D.R.E. with VVPAT that exhibits software independence as it's defined in the VVSG.

And if those systems were submitted to a

voting system testing laboratory today, and the testing laboratory did its job, it would not pass them.

And the reason for that is that all of the VVPAT systems -- I am not talking Op Scan -- all of the VVPAT systems, the VVPAT itself is created by software.

And in all of these systems, there is some code or some unreadable device that the human cannot interpret that tells whether or not his ballot is valid. And so if he can't tell that a valid ballot has been printed out, then it is not independent of software.

Furthermore, the idea that there is -- we're after this demonstrability, which I would love to achieve, but how can it be that having pieces of paper in boxes and rolls, which are handled by many humans and counted erroneously by any humans provide any kind of demonstrability that the totals in the election were correct. They haven't since the 1850's. I can't imagine what has happened in the year

2007 to solve that problem suddenly.

I agree that, to a certain extent, Op Scan ballots achieve software independence to a certain degree, at least to the extent that the ballot is not created by a computer and, therefore, is independent of software. I'll agree with that, but it still has all of the other problems.

So what I think, if we're talking about ghosts, chasing software independence as a

necessary aspect of a system for voting but not a necessary aspect of a system for anything else that we do, it sets an unnecessarily high standard that rules out all kinds of wonderful systems, including systems that have been fully operational for 25 years, all of a sudden they become unacceptable, because suddenly, we can't demonstrate that they work.

I don't agree that we can't demonstrate that they work. We may not be demonstrating it to a certainty. But certainly, looking at

appropriate testing protocols for things, it gets us to a sufficient level of certainty that the system has been working.

It always has. It does in everything else that we use in life. And so I don't understand why we have to produce 100 percent proofs of correctness for everything that is going on in an election.

>> KING: Thank you, Mike.

Peter?

>> RYAN: I would like to pick up again on this sort of avionics analogy, because first of all, to add to Ron's comment, the avionics failure is a manifest; whereas, there is no

God's eye view of what the outcome of an election could be. We can't just do an extrinsic check to see that the outcome is correct. That is one fundamental difference.

The other difference is how we can recover.

>> AUDIENCE MEMBER: Microphone.

>> RYAN: Sorry. Is the issue about how

you recover if you detect errors. If avionics goes critically wrong, you don't recover, and the plane crashes.

With the kind of software independence systems that some of us are investigating with voting systems, if you detect an error, you can potentially recover from it if you've got a suitable recovery mechanism. So I think that is another fundamental difference.

And so another reason why you need triple redundancy and so forth in avionics, is that you're going to have to go on the possibility that if things go wrong, you may not have a good recovery mechanism.

And by definition, if we're going to have proper avionics, the system is going to have to be software dependent; whereas, I think we

have -- as I mentioned earlier -- proof of concept demonstrations with voting systems, that we can have software independent systems, so there are all bunch of systems in which I

think the avionics analogy doesn't really hold water.

Yes, I'll oppose that.

>> SHAMOS: Well, if I can respond for a second. Give me 15 seconds.

>> KING: Go ahead.

>> SHAMOS: I actually agree that in avionic systems, that failures manifest. Yes, it is true. It is often if a plane crashes in the place where we can see it, then we see the wreckage.

But very often, the NTSB is completely unable, after years of study, to figure out exactly what it was that caused the plane to go down, whether it was a software problem or something else.

By the way, I am not arguing against redundancy or cryptographic systems. I was a big supporter of both here. I am with you on all of these things. What I don't understand is the requirement of software independence.

If you can achieve it, it is a good thing,

but requiring it of all systems is what seems to me to be unnecessarily restrictive.

>> KING: Thank you. Ron and then Peter and then we will wrap up.

>> RIVEST: I was just puzzled by again Mike's comment that D.R.E.s with VVPATs are not software dependent. I am wondering if you can sort of carefully delineate how an undetected able software bug could cause an undetectable change in the election outcome.

>> SHAMOS: It is easy. I will take a continuous rule VVPAT. The continuous rule of VVPAT. Every ballot image -- excuse me, cast vote record. Every cast vote record, there is a code printed with it so that an association can be made between that ballot image and the ballot image ostensibly stored in electronic memory so they can be reconciled. So what I do, if I have access to the software and I can be an intruder, an undetected intruder, what I do is printout a beautiful VVPAT for the voter that has identically his choices on the VVPAT. But the code that I print is an invalid code. Then when he leaves the ballot, when he leaves

the booth, I then printout another VVPAT that has the votes my software wants to it have and yet prints a code that says this is a valid ballot. I mark it as having been spoiled, for example.

>> RIVEST: I would argue that that is not a voter verified system. You have codes that unreadable by the voter.

>> SHAMOS: They are no voter verified systems because they all have unreadable codes on them.

>> RIVEST: You can write valid and invalid in English and then have the voter --

>> SHAMOS: Yeah, you can do that, but there are no systems in which everything on the ballot that can be used to invalidate the ballot is visible and readable to the human being.

>> RIVEST: I agree -- I am in agreement that system that does not have all of the important information that could validate be voter verifiable would not be software independent, that's correct. So systems.

>> KING: Let the record show that we have

25 an agreement. Thank you. Let's see, I don't

1 know who was up first, Alec or John? Oh, I am
2 sorry. Sarah.
3 >> JOHNSON: I have an easy question for
4 Peter. Specifically you had mentioned that you
5 have got some systems, proof of concept systems
6 that you are looking at, and obviously a lot of
7 this discussion is centering with D.R.E. That
8 is what we are talking a lot about. There are
9 thousands used and continuing to be used as a
10 speak in elections. Do you have the system
11 that you are looking at in England or other
12 entities, do you have D.R.E.s that meet the
13 type of software, the two different softwares
14 in one system that Michael was talking about?
15 >> RYAN: I think the first response is
16 the kind of system I primarily look at is not
17 really a D.R.E. system in that sense. It is
18 cryptographic, but it doesn't involve the voter
19 interacting with the D.R.E. touch screen or
20 anything like that. So I don't know, does that
21 answer your question?

>> JOHNSON: The question was a general question in general because we have got, do you have a system that can do this? We have got, no, you can't get it done.

My question was in general about your proof of concepts system that you have mentioned. Without going into a lot of detail, are they anything that we have seen today? Are they Op Scan? Are they D.R.E.s or are they something that is a hybrid that is something totally different?

>> RYAN: They are not D.R.E.s as a said. Yes, they are not. Keep it simple like that. I guess best described it completely differently. They are essentially cryptographic. They do involve paper trail of sorts in the sense that the voter does -- can in principle take away, well, I think Ron calls it protected ballot form which holds their vote in encrypted form on the form. And they can later check that that gets into a tabulation

process because a bit of mathematics going on there.

So there is a sort of paper trail in some sense but it is not, as it stands, a human readable at least at the point that it becomes the protected ballot. So human readable at the time that the voter casts the vote in ways I could explain later.

So again we come back to this issue that there seems to be some confusion as to whether software independence is synonymous with, well, VVPAT. Seems to be the implication. In my mind that is clearly not true, in the sense that I understand VVPAT. So yeah, but it is still quite theoretical. We have prototypes of it, and we have run a trial small scale student election trial with it last year. We will run more next year so the thing has been tested out. Does that answer?

>> KING: Okay. As we get ready to wind up this topic, I have got Alec, John, and the Juan. And if you could hold your comments to

may be a minute.

>> YASINSAC: Less than that. I had proposed initially that we talk about the properties that this persistent ballot need to have, the VVR, the IVVR. My contention is if you defined those properties and you defined them very explicitly in terms of what you needed to have to be able have a verifiable system, paper wouldn't meet it.

That is my contention, and I think that has been borne out of why we are where we are.

But since John is next, I will mention this as well, that software independence leans heavily on voter verification. Evidence is pretty good that voters don't verify their verifiable record even when they mark it themselves. It is debatable about how careful the average voter is in making their own marking.

So in lieu of that information, if voters don't verify the VVPAT and voters aren't across

the board careful in their marking of the individual ballot then where does that leave software independence?

>> KING: Thank you. John.

>> WACK: Just as a quick response, I don't know the percentage of voters who vote on VVPAT systems. I believe Op Scan in the last general election was 49 percent. And so I would just say there is a tendency to associate VVPAT with software independence, and I would sort of try to step back with from that. The VVPAT systems that were implemented to begin with I don't think were the best design and focusing on those tends to cloud the issue a little bit.

The other thing I wanted to point out that was something to Mike and Ron is that the TGDC hotly debated whether there could be anything on the paper record that essentially the voter could not verify or might be a secret vote that could be somehow or another changed in the electronic memory so that it would invalidate

the paper record. VVSG 2005 it had a requirement that said that the paper record ought to have a code or shall have a code on it that can link to its electronic counterpart. Some states require that.

The current recommendations basically said that has to be provided as an option. You have to be able to turn it off because some states regard that as a violation of privacy. There was also a lot of debate about whether there out to be any bar codes on paper record because basically a voter can't verify a bar code.

And the decision was that all paper records shall be produced in a way that they can be Optically Scanned which does not require a bar code. However, bar codes are allowed to be used most likely for the purposes of adding additional content to the paper record, for

example, if the paper record is going to be scanned and read back to a blind voter, perhaps the bar code could contain pronunciation answer

keys to candidates names and things of sort. But anyway, the requirement for linking the paper record to the electronic record was changed from VVSG 2005 from a I think should be provided as an option.

>> KING: Okay. Thank you and finally, Juan.

>> GILBERT: My comments are to summarize kind of these questions. I guess listening to Michael and Ron, one of the things that I clearly observe, and I like to bring this up and bring Brian in on my summary, which is, Ron said to his knowledge there is no software independence systems that use software as a back up or redundant observer. I think that there are examples of that, you know, there is one that we have worked on that uses video as a verification mechanism. And a novel way.

Other people tried it but they didn't use it a certain way. We hear Peter talks about one way to do software independence as well. As in the spirit of the VVSG and in the spirit

of the things we are discussing, we constantly talk about if you have something, we need to test it. We need the standard to test by. I think way have this innovation class which is outlined, but this is where Brian comes in. I think we should have some things to test innovation class itself.

There clearly are some things out there that people have experimented with, that people are trying, and I think these things will be excellent candidates to give the innovation class a trial. Looking at the definition of software independence, and straight from the VVSG, it clearly says that the voting systems software is not capable. So that begs the question is where is the boundary of the voting system software? So if I have one piece of software that in my mind, that is the voting system that is doing the tallying, that is presenting the ballot, doing those things.

If I have an observer, that is a piece of software. Now the argument becomes is that part of the voting system? Or is it an independent observer? So these are all questions I think that have to be answered, and

I think taking -- and this is just my recommendation, taking a few of these innovations that claim to be software independent and trying the innovation class, let's see if the innovation class will come out by trying in, quote, unquote, innovations and see if they meet these definitions. And so I end there.

>> KING: Okay. Thank you. I think I am going to exercise my privilege as moderator and we are going to take a break a little earlier than planned. I am starting to see fatigue or low blood sugar set in. But let's --

>> RYAN: Or jet lag.

>> KING: Or jet lag. Yes, Peter came a long way. Let's take a 15-minute break now, and when we come back, Alec, we will start with question number three and your lead in to that question. Thank you.

(Break)

>> KING: I think we are ready to reconvene if the folks in the lobby could come in and find a seat. We are missing two members

of the panel. Brian, did you see Sarah and Chris?

>> HANCOCK: Yes, let me see if I can go round them up real quick. Merle, also they are working on cooling the room off a little bit since it is warm.

>> Alec mentioned that he revised his documents. I am just wondering if those documents are out on the table, his revised versions?

>> YASINSAC: They are early versions.

>> KING: Carrie, you raise a good point. Maybe at the end of today, if anybody has updates to any documents they have submitted, they can identify that. Matt just informed me the other panelists are on their way, but they have given us permission to start without them.

We are on to the third question in the set of questions that we were asked to address. I believe that question is displayed on the screen behind us. "Do methodologies exist to test voting system software so it can be

reliably demonstrated to operate correctly? And then what added security benefits are created by S.I. that are not met by the testing process?" And Alec has volunteered to open with some guiding remarks on that.

>> YASINSAC: I would actually like to take this two directions. The first is to address the first part of that directly, do methodologies exist to test voting system? I think the answer to that fairly much an unequivocal no, there aren't ways to test the system to verify that it is absolutely correct and has proven that year after year after year.

On the other hand, software engineering has matured to the level that we are able to provide or the software engineering is able to provide high quality software based on mature software engineering processes, implementation of best practices, keeping of data that allow processes to be modified, to be able to repeat success and not repeat failure.

And I personally believe that this is the biggest omission, and it is not addressed at all in the VVSG. It doesn't mention any reference to the advances in software engineering to be able to leverage process maturity, be able to try and achieve the level of quality that would be incorporated into the voting systems that we need. And I will state strongly that any software that is involved in

a electronic voting system needs to be high assurance. It needs be engineered with rigor and it needs to be a software that has a lot of attention given to it to make it happen.

The second place that I would like to take this is actually to address something that Ron mentioned a few minutes ago about redundancy. It is actually a little bit of comparing apples and oranges of S.I. and testing processes. Because software independence really is not a testing approach. It is not a development approach.

It really is an architecture and that

architecture that provides the ability to have redundant mechanisms that can verify one another. And in this case, it is the mechanism that is the main parachute we call it, or I call it, is the electronic system and the back up parachute is the paper trail. And so that structure is inherently better in some ways than having an independent mechanism by itself that you try to engineer to a very, very high level of sophistication or very, very high level of assurance.

So what software independence has done is

provide this structure that has a bit more inherent security. Now, it is not without problems, and that redundancy specifically -- you have to think about the failure modes that those redundant mechanisms may take.

For example, in the case of the paper failure, in software independent systems, there is no redundancy. If the paper system itself is wrong at the beginning or is manipulated

before the election, so that we, for example, reverse candidates on some ballots or if the paper is manipulated during the voting process, or if the paper is manipulated after the voting process, there is no redundant mechanism, in general, that can generally detect that failure.

It is the redundancy of software independence, is exclusively the other direction. It will allow you to detect faults or flaws that are on the electronic side, but it doesn't really give you the redundancy that you would like to have on the paper side.

So on the flip side, if you do have electronic failure, then your failure mode allows you to detect some problems that you may

have in the election, and as have been pointed out, you may or you may not be able to trace that failure back to its cause.

And as was pointed out, if you can't trace it back to its cause, then in some sense, at least, the election fails, because one of the

goals of the election system is not just that it be accurate but that it be demonstrably accurate.

So if you have a failure, that you can detect that failure after the fact, and even -- I would contend, that even if you can make a strong argument about why the result was wrong, that first result being wrong is reasonable doubt to the candidate that lost and the folks that supported the candidate that lost.

So what software independence -- one of the things that it really does programmatically inject into the election system is the notion that that first count, if it is not perfect, that is okay, because we can fix it with a paper trail.

I think that is the wrong approach to take for election systems. If we have a paper trail -- and I am not against the paper trail.

The point is, if we're going to use it, we need to use it during the election period to have a

balance of mechanisms that -- that redundantly verify one another.

So that when we produce that election result on election night, it is verified, and it's correct, and it takes overwhelming evidence after the election is reported that there was fraud or whatever it would be to overturn that result, and that should be the focus, and that doesn't appear to me to be the focus of software independence. Yes, I believe that -- yeah.

I did also mention that the part of the redundant mechanism of software independence is audits, and audits, as was mentioned, they can't be required in the VVSG, although responsible election officials will do them.

I am not certain that it is possible for them to be conducted with enough rigger that this redundant mechanism is going to be as effective, as many people believe it will be done. So it certainly raises questions about the comprehensive nature of the redundant mechanisms.

And I, for one, believe that we should have redundant mechanisms involved to be able to verify these systems. I am just not sure that software independence provides it and it goes far enough from my perspective. So that is my opening comments.

>> KING: Okay. Thank you, Alec.

John?

>> WACK: If I can respond quickly in agreeing with many of the things you said. I recalled that there was debate during the development of the requirements for IVVR as to whether they were perhaps too design specific, did they -- did they basically mandate a system that you're going to do the auditing post election. You couldn't actually do it during the day so that, by the end of the day, the records could be -- the IVVR records could also be consulted and you could end up with verifiable results at the end of the day.

And this, as well as some other concepts, were debated and I think the general consensus of the TGDC was that we couldn't -- they couldn't write requirements yet to that -- to those sorts of approaches, and so that's, in a

sense, how the innovation class came about.

And so I -- I guess basically I am just saying that was considered, but then we had to get back to the real problem of writing a standard that is specific that doesn't constrain approaches too much, that -- you know, that people can actually write tests.

And there was a constant tension, in a sense, between what we would like, you know, versus what we know how to do. Some of these approaches were considered, but again, that is where the innovation class came in at that point.

>> KING: Alec, I had a question I wanted to follow on, looking back at my notes.

You said that if paper was to be used -- and I am paraphrasing, so correct me, that it should be used during the election. Do you recall your comment on that?

>> YASINSAC: Yes.

>> KING: If you could, amplify that a little bit.

>> YASINSAC: Well, it is the notion of a true parallel test. That notion being that, while you're conducting the election, while the

election is ongoing, you select random machines and you pull them offline.

And you use the paper trail -- you print the paper or if it is a paper printing machine or if it's a ballot marking device, you take it offline and you run it in essentially a realtime test of what the machine is doing. And then you analyze the results of that test of the paper against the electronic record that is created.

And you can detect -- in many cases, statistically, as Dr. Rivest says, you can detect, if there is an inherent fault in the software or potentially if there is malicious fault by using parallel tests during the voting day, as opposed to waiting until after the election is over to conduct audits to test the machines that have been used.

>> KING: Okay. Ron?

>> RIVEST: I just wanted to follow up with a question to Alec.

I like your concern for high-quality software engineering. I think that would be wonderful to try to improve the current state of voting systems by getting better quality

software engineering.

I am just wondering if you can say a little more about how you do that and how do you set up a certification system. When does a system fail because it has got inadequate software engineering standards somehow?

>> YASINSAC: The approach that I am advocating here is not to fail the product. What I am suggesting here is that we evaluate the process, which, again, is the way it appears to me that the industry is going, that you have a maturity level of your processes that is analyzed, via a standards body that some that are already in existence, to be able to determine how your organization produces

software.

If they exercise best practices, what the history of their development is. And we'll get, I guess, into OEVT later, but the OEVT can be added in here to be a cross-check in the VVSG process to validate and verify, I guess you can say, the level -- the maturity level that has been assigned to an organization.

And the OEVT will be able to give you a good indication of whether that organization

has quality software processes underlying the product that they produced.

It won't tell you exactly, but it gives you a pretty good idea. Again, saying this from having just done several of these things, you can tell a whole lot about the product -- the process by looking at the product.

If I might, while I have my microphone on, come back. I heard the discussion about not knowing how to write requirements for redundant mechanisms. I know it is difficult and I know it is not probably in the literature now on how

to do that. But I would contend that we also just don't know very much about how to write requirements for software independent systems, as I have raised before. In the VVSG as it stands now, there is not a mechanism in place that I can see that would allow me to take a system and be able run it against a processor, an algorithm, or an analysis and determine if it is -- if I present a system and say it is VVPAT, how does it become verified by the ITA? That it is actually software independent.

I think it is an objective process at this point. My point is, if the notion is we don't

have a good way to write requirements for independent mechanisms, that wasn't -- didn't appear to be anything that stopped the requirement to go to software independence.

>> KING: Thank you. Peter.

>> RYAN: Place the mic. Is that better?

So one important point which I think is maybe implicit in some of what we have been saying

is, as you all gathered I am a fan of software independence, in the sense we have explained. That doesn't mean that trying to guarantee high quality of the software that runs the election isn't an issue. Clearly we must be able to guarantee that the election will run smoothly on the day and techniques for robustness are still important.

We run it -- potentially there is a paradox to the shear transparency of the system that I have been trying to and software independent systems may act against it because the whole point is to try and detect any error or corruption that occurs and be able to correct it and so on. But of course the fact that it is done in a transparent public way may paradoxically undermine the trustworthiness of

the system. That is something we have to be very careful about.

So I want to stress this point that whilst I think as a design principle, the architecture of these systems, software independence is

crucial, but that doesn't mean we ignore the quality and robustness of the software. So I think that is one important thing. I can jump to your other point about how we might I guess specify the property of software independence. That actually strikes me that that is one of the easier things to do here at least in theory. And I think some of us could sit around fairly quickly come up with a full definition of what that means.

We compare to that some of the other tasks and challenges we talked about earlier about how do you set up a threat model and guarantee its completeness and so on and so forth. There are really major research problems and wide open issues in the security committee for decades and not ones we will solve in a hurry. But that one I think is actually one that is definitely doable.

>> KING: Okay. Thank you. John and then

Costis.

>> WACK: Just quickly, excuse me, responding to Alec. But in general, one of the problems with the VVSG is 600 pages and sometimes difficult 106, even if you have an active part in developing it. But I contend that it does basically quantify what software independence is and make it pretty clear whether the system you are bringing for testing is software independent or not. There is a very important chapter in there called the conformance clause and it is not a clause. It is an actual big chapter. But it pretty well defines the sorts of systems that can be software independent as those that use independent voter verifiable records.

And currently, those would be Op Scan or VVPAT. It pretty wall lays that out. There is a complicated, it looks like an Alexander Caulder mobile of bubbles called the device -- the class structure, the device class structure and it codifies this and it gets back to another point and that is that one of the biggest improvements that the VVSG represents is that it is made some advances on being

precise basically.

And one of big issues in its development was making sure that test labs and vendors agreed on what the system requirements are and how it ought to be tested. So that forced essentially writing to what people well understood and to a certain extent, that is, you know, that has probably caused some issues in that, you know, writing more performance-based requirements where things would be more difficult to test and would require more interpretation down the road. Might have been desirable in terms of making VVSG -- what am I saying here? Making it easier for newer technologies to conform. But it is the enemy of precision and that has been one of the big problems in the past.

>> KING: Costis.

>> TOREGAS: I wanted to bring back one notion that we touched on earlier in the conversation. That is the human element in the systems approach. And I have been reading and rereading that sentence, methodology exist to test voting system software, so we can reliably demonstrate to operate correctly. In my own

experience in complex software deployments have covered only about 20 percent or so of the investments made and the anxiety and risk profiles have to do with hardware and software. A full 80 percent have to do with the organizational aspects, the human dimensions.

And I know that it is kind of easy to sweep under the rug and say we will get to that later, but let's fix the machine part first.

But I constantly worry about being able to verify the correct operation system software at such a high level because all of us understand and enjoy the discussion and the collegiality that comes with software engineering and evaluations and so on.

But ultimately in some precinct, some polling station, somebody will be pushing a button or not pushing a button or reading some kind of an error message or not reading an error message. And I guess what I would like to raise is, is there a role for a prestigious

document like a VVSG to address that human component or at least put some bounds around it so we know if we spend so much effort trying to get to the inth degree or to the tenth decimal

point of accuracy and precision on the software reliability, if you will, that we somehow forget that there is a huge component that has to do with human dimensions that may perhaps throw our concerns out the window altogether? I don't have an answer for that. But I know I would love to have some kind of an annex to the VVSG that addresses the human components to answer that question about correct operation.

>> KING: That is an interesting observation because it certainly gets talked about. But whether it gets reduced into the document in a formal way, that is a very interesting observation. Mike.

>> SHAMOS: So I will propose to answer the questions that are on the slide. Do methodologies exist to test voting system software so it be reliably demonstrated to

operate correctly? Sure. Provided that you do it during the election. Parallel testing achieves that, properly deployed and administered. Some more interesting question is can you tell in advance that the voting system software is going to operate correctly? And everything depends on the meaning of the

word reliable. If reliably means can it be absolutely demonstrated to be so? No. If reliably means to a sufficient level of assurance to be able to be used in an election? I think the answer is yes, although others differ with that.

What added security benefits are created by S.I. that are not met by the testing process? The answer is there may be profound benefits, or may be no benefit at all. It depends on what the alternative to the software is. If the verification and auditing mechanism is more reliable than the software could have been, then you certainly have achieved a

benefit. If the alternative is less reliable than the software was, then you have achieved no benefit and in fact you have made things worse by relying on something that was less secure than the original. And as to the issue of is it easy to determine whether a system is software independent or not, I am going to venture to guess that it is touring undecidable to determine whether a system is software independent.

There are certainly cases in which you can

demonstrate that there is software independence. For example, in a case where no piece of software ever touches a document ballot, it is marked completely by human and tabulated completely by humans, that is software independent. On the other hand where you have document ballots of the nature of a VVPAT where there are markings on the ballot that are created by a piece of software, there are some things the software might create that might make the system not software independent

and yet on the other hand there may be ways of having software write something on a ballot in such a way that it really is software independent and I despair it being able to prove that. In any case, I still come back to the point that we have to look at what is the other thing that we are relying on if it isn't the software?

>> KING: Thank you, Mike. Sarah and then Daniel.

>> HANCOCK: Actually it is me. Because I don't have a name tag, I am using Sarah's. Sorry about that.

I just wanted to tag onto what Costis

brought up about the management side of things and VAC agrees with that 100 percent. And we are developing a set of management guidelines as a companion document to the VVSG and that was certainly the intent, they would be used together. We are currently in the second year of a three year initial development phase of

these management guidelines and certainly even after this initial development stage we will continue to look at the best practices out there to continue to increase and make this document more usable for election officials to get exactly to the goal that you stated.

>> KING: Good. Daniel.

>> CASTRO: I wanted to address a few points. One in terms of the idea of how can you reliably test if the software dependent system operates reliably? It seems within the VVSG there is already an assumption that there is a way to do that. And that is because when you talk about VVPATs one of the issues is how do you create an accessible VVPAT? Within the VVSG it is that you can use another software dependent system which would read back the VVPAT in audio version for the accessible user.

Now, how do you know the best word to correctly, obviously that is not software independent and there really is no way to do that in a software independent way. If you

want to say the voting is fair and uniform for all voters, then you have to be making the statement that, of course, that software-dependent component of the system is, in fact, as reliable as the rest of the voting system, so it seems like within the VVSG, there is already that hidden assumption that it is possible to have a software dependent system that is reliably tested.

I think there is another disconnect in the VVSG, and that is the idea of having open-ended vulnerability testing of integrity of the software.

Even though you're requiring software independence, there is many reasons to have open-ended vulnerability testing. I think that is a good idea overall. You want to look at privacy and availability issues and other issues that may arise.

If you're talking about testing for integrity, it seems like, why are you doing

that if you have the software independence within the system.

And, finally, I want to amplify a point I think we brought up a few times, and that is, as we talked about, many times voters are not verifying the VVPAT.

So by the definition of software independence, which is the voting system shall be software independent, that is, an undetected error of fault in the voting system software should not be capable of causing undetectable change in the election results.

So by that definition, if there is an error or a fault in the voting system software, and voters are not checking their VVPATs to make sure it is correct, then that is violating the idea of software independence.

>> KING: Thank you, Peter.

Ron?

>> RIVEST: I wanted to speak to these questions of the definition of software independence. You've raised some good questions about the limits of the definition and when it applies and what counts as software independent.

In part, the question is, what is the most useful definition of software independence, and you need to have a precise definition for testability, of course, too. So with the two issues that were raised -- one is the voters not checking.

So if a voter does not check his printed record that he's got if it is printed out, say, or whatever, it remains as software independent, because it is detectable.

"Detectable" meaning capable of being detected. If the voter is not looking at it, of course, then he is not detecting it, but it is still detectable.

So it's just the fact that the voters don't look at -- the output wouldn't violate the definition of S.I. So you can't put a standard in place that requires the voters to do certain things and so on. It is only about the equipment, so you just have to say it supports the detections of those kinds of errors.

So S.I. does not require that the voters look at the ballots, and of course, it can't.

25 You can't pass a system or not depending on

1 what voters are going to do.
2 And with respect to voters with
3 disabilities, you get into a very
4 interesting -- if you have a blind voter, of
5 course a blind voter can't look at their
6 ballot. And so then the question is: Is this
7 going to be SI or not?
8 The intent is that a system should not be
9 able to tell if a voter who is voting is blind
10 or not. So if a voter is using an interface
11 that is designed for blind voters, but if a
12 poll worker goes and votes as if he were a
13 blind voter and sees the printout himself, then
14 the error is detectable, and that would qualify
15 as S.I.
16 If the voting system knows for sure
17 whether the voter is blind or not, then, in
18 fact, it may not be S.I. because the voting
19 system could change the votes of only the blind
20 voters. But if the voting system can't tell if

the voter is blind or not, then you can have a system, which is S.I.

We're getting into the fine points of the definitions here. They are interesting questions. But the question basically: Is

there evidence produced by the system that would allow an attempt to cheat, attempt to defraud somebody, or disenfranchise somebody?

The example that Michael had: Are those going to be detectable in principle, and whether they're actually detected or not is a separate question.

>> KING: Peter and Juan.

>> RYAN: First of all, I wanted to agree with Mike that, yes, clearly, you have to look at the rest of the system to see whether dependency is thrown if you move it away from the software. And people are doing that.

We are looking -- taking this sort of system, a wider view of the system. So that is something which is taken on board and people are working on that.

One other comment I wanted to make about this one about the assumption or having to depend on voters performing various checks. That is one thing that people recognize that could be an issue, and so we have looked at other alternatives, so you can supplement, for example, voter checks by other kind of checks.

So one of the ideas that has been

suggested is to have sort of a verified encrypted paper trail, a sort of additional copies of these protected ballots that is kept, say, locally, so you can have independent auditing authorities also making checks at the cross-points between that and, for example, what is published on the web bulletin board that goes into the tabulation, or having voter assistance organizations, they -- who can vote, for example, pass their ballot, their receipt -- protected receipt to their local representative who could do the check for them.

So there are ways you can supplement the

voter, the dependence on the voters by other mechanisms if you're concerned about that.

So I think that is my point, yes, and there are serious issues, but people are taking those on board.

>> KING: Juan?

>> GILBERT: I think there is definitely other ways to do this. One thing would be a multimodal approach. So getting at the idea that you have one system or one interface that everyone votes on independent of ability, in that case, what a sighted person does would be

similar or the same as one who is blind, if you have an interface where you can accommodate multiple modalities on the same system.

Now, the system can't treat one group any different because you don't know who is going to vote how. So a sighted person could vote as a blind person.

And these kinds of approaches, I think, that gets to something, I think Daniel was bringing up, which is you actually do have a

sense of being able to test and get a verification that is equal across for everyone.

That should be our goal, and we are not here to talk about usability. I understand you have a different panel to talk about that.

But I think it is kind of -- the two go together from a usable security perspective. I mean, the ultimate secure system is one that no one can use.

I can secure it in such a way that no one can use it, I can guarantee it is secure, but you lose usability, and I can make it so freely usable and accessible, that it has no security.

So I think, in a sense, those two go hand-in-hand, and those two have to be

considered simultaneously. Otherwise, you're going to shorthand one or the other.

>> KING: Thank you.

I have a question for Chris and Sarah, and it is going back to the first one up there.

If you could consider from either a state

jurisdiction or a county jurisdiction perspective that ties into a comment that Mike made earlier about mitigation of risk occurring at different levels.

So the question that I have is: If, in the final version of the VVSG, whatever software testing methodologies are implemented, do you see -- among your peers or among your own colleagues in your jurisdiction, do you see the development of methodologies at the state or at the local level to perform testing of systems that may pick up any residual risks that are in the systems once they're passed through the federal certification?

>> THOMAS: Well, there has been discussions of doing post-election auditing, of course, as one way, and the issue of whether the voter verifies their ballot or not, I mean, really all of this plays out in a political

world.

And the political world generally knows when an election -- when election results don't

conform to a norm that is expected, and that's when I see the VVPATs coming into real play, is at the recount.

That is where you're going to be comparing what the machine says -- the software says compared to what all of the little pieces of paper said, as difficult and onerous as that may be. So that is an element.

Now, state certification of systems after the federal system is kind of all over the map. There is not -- I don't see a lot coming out of states that I am aware of. You see what California has been up to, obviously.

But that is doing much more than once the system passes, other than to see that it conforms to the actual state statutes and that it conforms whatever may be unique or not tested at the federal level.

Obviously, there is the accuracy tests that are done. There is pre- and post-accuracy tests, and then there is auditing. And that's sort of -- the auditing is the next frontier.

Michigan has got one of these pew grants to work with, Maryland and, I believe, Utah, to come up with some documentation on post-election auditing. But beyond that, I don't see a lot coming out of the states.

>> KING: Thank you. Sarah?

>> JOHNSON: I agree with my counterpart. I don't see a lot coming out of states, not because there isn't a desire or recognition of how important this issue is. Not at all for that reason. The reason being in most state agencies that do elections and state boards, in my case that do certification, the expertise isn't there. We don't have the expertise. We don't necessarily have access to the scientists and to all the expertise.

And I am sure Alec can talk about the money -- the project that it took for Florida to do their test. California spent over a million dollars, etcetera, etcetera. You have got the timing issue and the money issues that all do factor into it.

I don't see a movement that states are going to start doing more testing or reinventing the wheel. I think there is

already a reliance on the federal testing system. We have all learned a lot about what that testing system was or isn't, so to speak, but I just don't see the move because of the expertise and the money. And we rely on our state legislators who view or don't view this as an important issue to do beyond what the federal does.

>> KING: I have a follow-up question, Ron, and then I will turn to you. John, in the discussions at NIST, is what Sarah talked about factored into the scope decision on the VVSG, the fact that if many states are simply accepting federal certification as the defacto state certification that that places an additional level of expectation on the federal VVSG?

>> WACK: That -- I don't know how best to answer that.

>> THOMAS: The answer is yes.

>> WACK: To a certain extent, I would say that the big area where I heard discussions was really more in additional testing that states

24 are doing on top of federal certification

25 testing. And that some states were actually

1 doing some fairly expensive expert security

2 reviews and additional banging away and in

3 finding some real problems, finding some fairly

4 significant problems and issues that would lead

5 them to wonder why the systems passed the

6 certification test to begin with.

7 And that this was expensive and if the

8 VVSG could essentially set up a system so that

9 the conformance testing to the VVSG would in

10 itself sufficiently rigorous, states may not

11 have to do additional testing. Or may not have

12 to do additional testing to the extent that

13 some states were doing. So that it might be

14 ultimately less expensive to have a more

15 rigorous VVSG and a more rigorous performance

16 testing process that, ultimately, you know,

17 those savings would be passed onto states. I

18 don't know if that really answers your

19 question.

>> KING: John, does rigorous there imply depth, more breadth or both?

>> WACK: Well, I would say that both. Breadth in terms of volume testing. Previous versions of the standards allowed bypassing certain parts of the system in testing. You

could hook a test harness up to the system and bypass the user interface and not have to test that to the same extent.

Some of the accuracy tests were specific accuracy tests, and the new approach is really to in essence, like I said earlier, conduct the mock election and pretty much have live test subjects banging away on systems for a period of time, starting with the user interface and ending up with making sure that you are getting usable records out of the voting system. So that is the breadth.

The depth, to a certain extent is handled in the usability performance testing for accuracy. And open-ended vulnerability testing, I have sometimes wished that it had

been called an expert security review because I think the open-ended part of it leads people to believe that it is, in a very expensive open-ended process that will never end. But it is an expert security review that in essence allows people to dive down into the system if they need to find out if there are any issues. So I guess my answer is, I think to the extent that people could, they try to make it wide and

deep.

>> KING: Okay. Thank you. Ron.

>> RIVEST: I think John actually made most of the points I am about to make. But I just wanted to emphasize them a bit. I think one of nice things about the new VVSG is the volume testing that is going on. It really is running a mock election as John said, and I think that is a major help in trying to weed out systems that are unreliable when you have got frequent printer jams or other problems. I think that just running a heavy duty mock

election with real equipment with real voters a major improvement.

And I think it is modeled, back to the question of tension between the state and federal -- or not tensions but cooperation between those two, it really is modeled after the California volume testing. So the states are leading the way in some of these things I guess is where the federal government is, adopted and picking it up and saying volume testing is a good thing to be doing here.

>> TOREGAS: If can I ask a clarifying question. Have the legal people opined about

liability, shared liability, if state or municipal government, county government assumes that a test that was done at the federal level would ferret out all of these inconsistencies and in fact was proven not to? What happens? I am sure there is an easy answer to that but.

>> KING: I will defer that to counselor Shamos.

>> SHAMOS: There is not an easy answer.

What happens is we had an example of this in Pennsylvania where a system that had been certified was suddenly decertified when certain flaws were pointed out by citizens. A re-examination was conducted and was decertified. That was easy to do. Then the counties that had purchased the system showed up at the door of the secretary of the commonwealth and said, we need money to buy another system that you said was certifiable in place of the one that you originally said was certifiable.

And in that particular case the number of counties in which the system was used was small enough that the secretary was willing to pay the freight. But if half the counties in the

state had used that system, we would still be in litigation over it.

It is absolutely unclear whether there is -- could be any liability on the secretary of state for carrying out secretary of state's

duties. Could there be any liability on for example the consultant to the secretary of state who actually performed the examination? I shudder to think.

>> KING: Alec.

>> YASINSAC: I just wanted to follow-up. I think there is a bit of a misconception about the OEVT and what has happened in the states. To my knowledge, no state does OEVT testing as part of their certification process.

The TTVR in California was all systems that had been in use and the question was decertification process, not the certification process where the plan was laid out ahead of time. I think this is a critical point because in the future it was -- it is actually fairly easy to find flaws when nobody knows you are going to be looking for flaws.

Once this notion is applied and once if it goes the way it would -- would be most

beneficial in my belief, then the process would mature so that the OEVTs are guaranteed to find

things. I mean, it would be hard to put together a team almost with the systems that have been out there. They won't find faults in the process, the TTVR, the Florida studies, there have been things that have found flaws because the systems weren't engineered to be able to defend against that type of analysis.

It was done after the fact and so it was very easy to find those faults. So the next thing we have to look at is what happens when you do an OEVT and don't find faults? Then that is the big question there. But it is not exactly an implementation on what the states have done. It is kind of a reversal that says we need to do it up front and hopefully that will impact the process.

>> KING: Ron.

>> RIVEST: I was referring to the volume testing California does, not the top to top bottom review. You are absolutely right that that was post facto. The volume testing I believe in California is done before certification in California. But I may be

mistaken on that.

>> YASINSAC: I am not sure.

>> TOREGAS: One more question. One more quick question. Again, to signify my ignorance. Where is the industry in all of this in terms of demonstration of reliability and so on?

I presume that there is a certain finite number of companies that are involved in this business, and I, again, presume that the VVSG is ridden with an eye towards the industry itself. Can somebody kind give me an idea of where the industry is in terms of their current ability to demonstrate correct operation and their ability to operate correctly under the proposed VVSG?

>> KING: Well, there are no vendors present at the table here.

I don't know, Brian, is that something you want to comment on in term of the vendors' roles in the VVSG?

>> HANCOCK: Well, the only comment that I will make is the structure of the TGDC was laid out in the Help America Vote Act, as we all know. And as TGDC is constructed, there is no

vendor involvement at the table, although certainly in 2005, we received numerous comments from the vendor community, and we certainly expect to receive at least as many, if not more comments this time around.

>> KING: Yes, I think cost is something that you mentioned earlier, and we've had some side conversations about, and that is: Who are the stakeholders in this process?

And obviously the vendors are a stakeholder. But then the follow-on question is: What is their role? What is their responsibilities? What is their accountability? What is the state of the practice?

Those are all related to that essential question of who are the stakeholders.

>> TOREGUS: I guess the reason I ask it is not because I am speaking for the vendor community. I am not, because I don't belong to the vendor community.

But if I had a 25-year-old son -- I have a

20-year-old son, so I am getting there -- if I had a 25-year-old son. And he said, Dad, should I go into this business? Is this a good

business for me? Is this an entrepreneurial business to get involved in?

And having heard this discussion and having read some of the materials, I would say, boy, that is a real rough area to promote to my 25-year-old son.

If I am the secretary for economic development in the state or at the federal level, and I want to promote and to strengthen industry, it's part of the harsh balancing act between standard setting organization that tries to develop kind of aggressive and correct things, but at the same time, be able to find the actual product in the marketplace.

And unless the states and localities of the federal government is prepared to manufacture these things, we also have to give ear to that. I hear your discussion that,

historically speaking, they have not been given a place on the table.

But ultimately, there has to be some kind of an intervention, some kind of listening ear, and I would suggest that would be useful again, part of the expanding communication for this discussion.

>> KING: And well said.

John?

>> WACK: I had one other comment, and that is, the question up there, "Do methodologies exist to test voting system software so it can be reliably demonstrated to operate correctly," was -- that question was pondered a lot.

Actually, one of the people working with NIST in the TGDC went down the route of essentially wanting to develop systems in such a manner that they can be proved through some sort of a fault analysis to be correct, and they, you know, possibly may not require any sort of independent record. This analysis

would be sufficient.

And the little I know about this area -- I know it is pretty foolhardy to talk about something you don't really know a whole lot about in public. I think peter Ryan knows probably more about what I have to say than I certainly do.

But if you are going to basically develop software that you can test to reliably demonstrate to be correct, you have to develop

it in a way, in a very specific way, such that it can actually be tested. So you probably have to use very formal methods, which the DOD and I am sure the airline manufacturers use, to develop software in very specific ways in which it can be more easily tested.

And ultimately -- you know, the E.A.C. ultimately has to end up with a document that testers can very clearly read, and it can't be fuzzy testing. It has to be fairly specific testing. It has to know what passes and what

doesn't.

So the reason I say that basically is we could have gone down that approach with the VVSG, possibly, and really upped the way in which software was developed and specified it and possibly could have made it easier and more accurately tested.

However, that would have come at great expense, quite a bit of an expense. It would have taken much longer to develop the VVSG, and it may not have been something that the vendors would have wanted to accept, because they would have had to change their software development practices in a big way, and it would be much

more expensive for a vendor to get into the business than currently.

So, basically I bring this up just to say that, yes, I believe there are methodologies out there to test software to reliably demonstrate whether it is correct, but it means that it has to be developed in specific ways to make that possible, and that will be very

expensive.

>> KING: John, thank you.

I wanted to make a comment that ties together John and Alec's observation about the possible challenges of applying open-ended testing to products that were not designed to sustain that kind of scrutiny.

And John said we need to be looking at how the VVSG and its implementation impacts vendors coming into the market space. And I think for those of us who rely upon these vendors, I think there is an additional issue of having those vendors stay in the market space.

And one of the concerns that is expressed often by election officials is: What are the contingency plans if vendors decide that they are going to move their resources into other

markets, that they may be more competitive in?

So I do recognize that the folks that are crafting the draft of the VVSG do think about the vendors' role and often think about it in a

way of just trying to understand the vendors' role, and sometimes the vendor doesn't fully understand the vendors' role, it seems, so a very complicated problem.

I would like to move on now, if we could, to the next question on the list, question number 4: "What are the relative merits of the various types of direct, that is by the voter, and indirect by automated system independent verification techniques?"

And we didn't have a volunteer for there, so I will make a few introductory comments, and I'll turn it over to the other members of the panel.

When I thought about the direct verification, there is a lot of benefit to having the voter directly involved in the verification of the ballot.

One is that the verification techniques can be very intuitive, may require a small amount of training and/or easily understood by

the voters, that is, what they're verifying.

The second is that they can be realtime, and in transaction processing systems, we often talk about the inherent challenges of pre-editing and post-editing.

And that is, when you can pre-edit data, that is, get the right data, correct data into the system, it optimizes the processing and minimizes the need for exception handling.

On the other hand, if the edit is kind of post-processing, that involves not only methods of handling the air conditions of the anomalies, but then you have to have a method of verifying that the verification has, in fact, occurred and any changes have been done properly.

So some questions that I wrote down is: Can correct verification approaches be enhanced by better ballot design? And again, I think in part that is a usability question and an accessibility question.

But, I think, also, when we ask voters to verify what they have done -- we have heard on this panel and other discussions -- that voters often do not verify. They don't consult the

VVPAT, so is that possibly -- instead of sometimes it is assumed to be an issue of voter disinterest, could that be issues related to ballot design? Could it be issues related to navigational schemes within the system, related to voter education initiatives?

One of the things that we -- we often talk about, is one of the holy grails in voter verification, is the notion of the secret ballot.

And my experience is that there are a lot of different ways that we define the secret ballot. Some of it is a technological definition. Some of it is certainly a legal statutory definition.

But do we have consensus on what we mean by secrecy of the ballot? And even when we talk about the ballot, verifying -- verification of the voter's intent, verification of the voter's choices, verification of the voter's tabulated choices, there is so many different dimensions to that that again, a theme that I have heard here today is that perhaps a lexicon in models would

25 be helpful in reaching consensus. The indirect

1 methods of voter verification obviously
2 introduce a different system, whether that
3 system is manual or automated or a hybrid of
4 that. And when we introduce an additional
5 system then we have all of the uncertainty that
6 a new system creates not only its inherent
7 functionality but its interfaces to the
8 existing system become source of risk.
9 And my final question that I have to help
10 the panel kind of form their responses is going
11 back to something that Mike said and I said
12 earlier and it deals with reasonable assurance.
13 When we are talking about verification, whether
14 direct or indirect, what is our target? Is it
15 our target that absolute zero uncertainty or
16 are we moving toward discussions of reasonable
17 assurance, reasonable test and what might those
18 be? So with those comments to kind of help us
19 form some questions, I will turn it over to the
20 panel. Mike.
21 >> SHAMOS: I will plead again for some --

a definitional beginning of exactly what we mean by verification. So I think what most voters believe is going on with their verification is not what is actually going on.

There is a common phrase that is used but voters want to be sure that their ballot was counted as cast. That is the phrase. Counted as cast. There is no system currently that provides that kind of verification, except the cryptographic ones. I am talking about the commercially available systems do not provide that. What they do provide is a verification that the system correctly captured the voters intent. Because if the system is able to capture it and spit it back out to the voters so the voter can check and see that all the selections are the ones the voter wanted to make, that indeed demonstrates to the voter that she was heard correctly.

As to what happens downstream, the voter does not have assurance of that. In fact, we

want to make sure that the vote is counted correctly. We want to make sure that whatever record is made of the vote is sufficiently permanent, that it still exists not only at the end of the election but at the time of any audit or recount. And we want to make sure and this is virtually never spoken by anybody, we want to make sure that no unauthorized voters

voted in this election because it doesn't do me any good if I know that my vote was counted if ten people vote for every living person, then it doesn't matter whether your vote was counted correctly.

And further more, all of this stuff needs to be able to verified by the voter after the election is over. And typically, what the VVPAT provides is the first form of verification, which is the system heard me correctly. So in answer question four, I am interested in exactly what kind of verification are we talking about? And my preference would be for end-to-end verification. But there are

no commercial systems to provide that.

>> KING: If I can ask just the following question. Mike, do you think there are legal barriers to that end-to-end verification?

>> SHAMOS: No.

>> KING: Okay.

>> SHAMOS: I think what you are saying is, if the voter can satisfy herself that her vote was counted then it seems to stand to reason that she ought to be able to prove that to her neighbor that her vote was this and

counted that way.

But there are cryptographic systems that permit solo verification without the ability to prove to someone else how the voter voted. So was that the concern? The secrecy? Also I agree we need a definition of secrecy. Secrecy seems to mean two things. To some people it means that no one else can find out how the voter voted without the voter's permission. And to me, what secrecy means is not only can

no one else find out, but the voter cannot demonstrate to another person how she voted. And I think those are often intermixed, and we ought to keep them straight, secrecy one and secrecy two or something like that.

>> KING: Thank you. Ron and then Peter.

>> RIVEST: Thanks. I think Mike started off on a good direction here. It is often helpful to have clear definitions as to what is being verified and what we are talking about and I agree with everything he said on those points. Just to try to clarify some of the potential distinctions one could make, when I talk about things that might be verified in voting I tend to make a following three-way set

of steps that need to be verified which are pretty much -- first is cast is intended. Is the vote captured correct? Did the vote get correctly captured. That can be direct or indirect as we have talked about. So cast is intended.

And the second step which is often skipped

as collected as cast. So usually there is a process of collecting the records before they are counted so are they properly collected? Is there -- and some of the end-to-end systems have a formalization of that process where in fact all of the ballots that were cast encrypted form to the website so you can actually see the collection and you can verify that a particular ballot is present in that collection. So verifying that they are collected as cast is a verifiable step in some of these systems.

And then finally, you have the step counted as collected. So you want to verify that the tabulation is correct. That is interesting if the ballots are encrypted of course, but there are ways of getting around that. So count cast as intended, collected as

cast, counted as collected I think is an interesting and useful set of distinctions to make. The issue about no dead voters is

probably the one of collected as cast. I guess you have got things in the collection which correspond to things that weren't cast and so have to go there. I think the best way to do that is to post a list of the voters who allegedly voted and have other citizens be able to check that and say, you know, this person didn't vote because they are dead or something. But that is a hard one.

>> KING: Okay. Thank you. Peter.

>> RYAN: Well, I agree very much with what Mike said and what Ron just said. I want to follow-up your comment about the secrecy. That is a very good point and people have recognized that and there are at least three different flavors which correspond I think very precisely with what you just said. Privacy in the naive sense, a passive adversary, and there is an even more sophisticated one called cohesion resistance so that has been taken up and people have come up with precise definitions of these different

characterizations of security. So that is a good point.

Yeah, I would just like to echo what Ron said and the way I would like to describe some of those cryptographic systems as they are in the sense three stages in which the counting, collecting, and counting of votes that can go wrong. First in the encryption or encoding step that things can go wrong and then sort of transmission into the tabulation phase, and then the actual tabulation and encryption phase. So you have to look at all three of those and make sure that there are ways to do checks and balances to make sure that any malfunctions at any of those stages can be detected. So that is in essence what is going on at a very high level.

>> KING: And Mike, if I am not mistaken, there are jurisdictions where the vote of the dead can be counted depending on when they cast it in early voting. So you may need to expand that explanation. I wanted to pose another question to the panel that is related to this. And I think it is a good question because it doesn't have an obvious answer. And that is,

can mandates produce technology? And this has come up on a couple of different discussions.

>> SHAMOS: Mandates plus money.

>> KING: And if it can produce technologies, are they appropriate technologies? And by that I am always looking for the application of the law of unintended consequence. So as we look at the VVSG and perhaps other things that kind of swirl around federal issues in election technology, be interested in the panel's thoughts about the efficacy of mandating technology and evolution through statute or through incentives plus statute and whether there are any potential unintended consequence of that. And I can't tell if these are up for this question or for -- okay. Mike, go ahead.

>> SHAMOS: Unintended consequence. So when VRE machines first came into use in the early 1980s, almost all states that allowed them had a requirement that they had to maintain a paper record of vote, individual cast vote records. And the vendors recognized

24 at that time that it was impossible to maintain

25 that record in sequential form where it -- or

1 would be possible to tie a particular cast vote

2 record back to a particular voter, so various

3 randomization techniques were used, and they

4 were used consistently in all D.R.E. machines

5 until after the year 2000, when the call came

6 for voter verified paper records and the

7 vendors saw that they had a sales opportunity,

8 they threw away absolutely everything they had

9 always understood about the need for

10 randomization and immediately came out with

11 inexpensive, sequential paper rolls, which they

12 knew they couldn't use, but nonetheless, it was

13 a solution to a mandate, it was a solution to a

14 problem, and look what has happened. And now,

15 they're all over the place.

16 And so the unintended consequence is that

17 some people have woken up and said, wait a

18 minute, this violates voter privacy, we can't

19 ever actually let anybody look at that

20 sequential paper trail, or it will violate

voter privacy.

So it is stored away in a safe, and nobody ever gets to use it. They don't use it for audits. They don't use it for anything. I think that it is a highly unintended

consequence, but it is because the vendors were forced to do something very quickly to respond to a perceived market need.

And everybody threw away the cautions of the past and allowed them to do it, and then actually bought the systems and then actually used the systems.

>> KING: All right. Thank you, Mike.

Any other discussion on this question? Yes?

>> THOMAS: I just agree with Mike. I think that as this political process moves down the road in terms of defining what these systems do is, watch out what you're going to get, and I think also watch out for undermining further any confidence that people are going to

have.

The more this goes down the road, the more discussions that are out there and kind of all of the boogie man stuff that goes on with it. It is doing an incredible job of undermining things.

>> KING: Costis?

>> TOREGUS: A reaction you provoked with your question, and then something else. In

other sectors when we think about new technology, there is usually an opportunity to do what the social engineers would call "business process re-engineering."

In other words, look at the process as it existed before the new technology comes on board, and then have a chance to change the process because of what the technology enables you to do.

It appears to me that in this particular sector, election technology sector, we're trying to kind of have our cake and eat it, too. We think about innovation, maybe some

changes, but it is usually at the fringes.

I would be hard-pressed to remember a paper I read or a product that I saw in the marketplace that makes fundamental changes to the process itself.

And of course, we could quickly say, well, the process is sacrosanct. This isn't the law. This isn't how we do it. And yet, in many other areas of government, we have found ways to modify the process and take advantage of the existing technology.

For me, at least, I find the technology of

elections has not yet matured enough, perhaps, to be allowed to enter this realm of thinking of business process re-engineering, and perhaps that is something to be considered in the fifth question, we talk about the innovation class.

The other comment that I have is with these kind of evaluations and verification and so on. After a certain point, we have to also begin to think about how the voter thinks.

And I have to be honest with you as a voter myself, I would much rather go to an election place, cast my vote, and have the confidence and the expectation that the system that receives my vote, the public administration system behind that process is strong enough, transparent enough, and professional enough to take care of everything else. It is a hope.

But in a sense, here we are, trying to manufacture the technology component to do something that perhaps we ought to be looking at strengthening our public administration system that could then run circles around what a simple machine can or cannot do. That is a bigger, a higher level of expectation that

perhaps some other group needs to be thinking about.

>> KING: Yeah, I am going to take this opportunity to plug the management guidelines effort of the E.A.C., which I think that's a fairly good description of what the goals of

that process is.

Dan?

>> CASTRO: I just wanted to add on to what Mike said earlier about can mandates produce technology, and, yes, but the funding doesn't matter.

And I think it is interesting, because with voting technology, the way we're setting the standards here is very different than what you see in a lot of other industries.

For example, in the auto industry, when they're setting fuel efficiency standards, that is set for cars that will be developed in the future. It is not imposing any kind of standards on the existing technology. I think it is very important when you talk about setting standards that don't have any -- any funding tied to it.

I also think it is important, before you

set those standards -- maybe there is a need for it -- but when you decide that there is a

need, you have to be deciding that based on a clear risk analysis, which is what we originally talked about. You have to say this standard is this much measurably better than what we had before to justify that kind of cost.

>> KING: That is a good point.

When I was formulating the question on -- you know, can you guide the evolution of technology with mandates, I did think about the fuel efficiency and the '73 Pinto and '74 Vega, and I do have concerns about how effective it is to mandate the development of technologies.

I think what I would like to do at this point is, I am looking at the -- at the body language of the panelists, and I think it is time for another break.

And I would like this 15-minute break to be a little shorter than the last 15-minute break, because we do -- we still have another question, and then we have some summarization to go through, but I do think people need to stand and stretch, particularly up here up

front.

So if we could, let's take a hard 15 and --

>> AUDIENCE MEMBER: What time do we have to be back?

>> KING: Good point. I have 4:25. Let's be back at 4:40.

(Recess from 4:25 to 4:40 p.m.)

>> KING: If we can take our seats please. Before we start in on the fifth and final question, I wanted to kind of recap the agenda and where we need to go and what we want to try to finish up in the next hour or so. After we have addressed question five, we have left enough time in the schedule to come back and really maybe tease apart some of the points we looked at earlier that perhaps subsequent discussions of questions illuminated something that we want to go back through and review.

And then before we leave today, we have got an opportunity for every panelist to make a closing statement. And my intent there was usually when I am giving a lecture, there is two or three things that I want to make sure that the students walk away from and often I

refer to those as just the take away. So there will be an opportunity at the very end for each of to us pass onto our colleagues on the panel, pass along to the E.A.C. Standards Board and to pass on to the E.A.C. commissioner the things that we really would hope that will be persistent from this meeting and merit further attention and perhaps further discussion at subsequent meetings.

So I am going to -- Peter, I am hoping that your biological clock is revving up around now. Mine is starting to -- well, that you are on UK time. No. I am sorry, it is very late, isn't it? But Peter has volunteered, and we do have question five up there. He has volunteered to lead us into opening discussion of that question. So if you would. Oh, you thought you had? Then I accept your withdrawal. I am sorry. We had discussed this earlier. So I will do my best to get things started but jump in and help me.

The question is how can innovative systems

be evaluated for purposes of certification?

And some follow-up questions about how do other

industries deal with testing and certification

of innovative products? And this is I think

directed towards the concept of an innovation

class as an alternative way of introducing

systems into the VVSG certification process.

Do we create unintended back doors for the

certification process and again looking ahead

at potential unintended consequence? And then

can a set of limited standards be created in

order to make the path toward certification of

innovative systems more clear?

And I think in looking back at the 2005

VVSG, I had an opportunity to work with the

E.A.C. on the collecting and cataloging of

comments. And I can remember distinctly there

was a day about 45 days out from the end of

comments where I was asked, you know, is there

much activity? And the answer was no, it was

just some people are responding. And then as

people really thought through the implications

of what was in that document, it accelerated. And then as a function of that acceleration, other people saw the comments that were being posted and that inspired additional lines of thinking.

So I know that the authors and the TGDC

and the Standards Board are all concerned that as this document goes forward, that due diligence has been done on thinking through unintended consequence. We have got always the mandate that we have to live with these documents for whatever their life is. And so I think with that as an introduction about how is innovation managed perhaps in other industries? Are there models that can be looked at? And does the innovation class proposal create a potential back door to the certification process? And then finally, is there potential limited set of standards that could accommodate the innovation class approach?

>> SHAMOS: I have now forfeited my right

to talk.

>> KING: I have been waiting all day for that to happen. Recognize my -- go ahead.

>> SHAMOS: So I am not a fan of the innovation class or the name innovation class. So in fact I think it is a proof that possibly too much of the VVSG is design oriented rather than functional oriented. Because if it were truly functionally oriented then anybody could propose a system for certification, and it

would be examined to see if it performed the necessary function.

If one of functions is software independence, fine. If one of functions is that it must provide verifiability at certain levels in the voting process then fine. But I think what is going on is the VVSG has anointed VVPAT systems as the ones that satisfy the requirements. And if you are not a VVPAT, then it is your obligation to show up hat in hand and prove to the examiners that your system indeed satisfies these functions.

And I don't think there is any reason at all to make that -- to make that distinction. It is conceivable that somebody could come up with a system that didn't fit into the VVSG at all. Hypothetically, suppose I had a reaping machine that was able -- I could point it at your head and determine from that how you wanted to vote. Such a system, frightening though it might be, if it were submitted for certification I don't believe it could be tested to the 2007 VVSG which doesn't even contemplate such a thing.

Okay. But yet, the systems that we are

talking about, for example, the prime three system at Auburn, is perfectly consistent with the kinds of voting systems that we have seen before and doesn't need to be sent to the back of bus in the innovation class.

As far as whether a certification process for innovative systems is going to be a back door, I think it is quite the other way around.

I think that the -- that what happens in these so called innovative systems -- and I am not sure what you mean by innovative. I think it was an effort to sugar coat what was really going on. But let's take it at face value and if these innovative systems were truly innovative, that is they incorporate new ideas and new ways of achieving security, new ways of achieving assistive voting, new ways of achieving verifiability, then it certainly isn't going be a back door that will allow these fundamentally bogus and substandard systems to somehow get into the elevated class of the VVPAT. It will not happen that way at all.

My belief is that these systems will end up being better, and it is not a back door.

And in fact, the VVPATs that have already taken the back door. And so can a set of limited standards be created in order to make the path toward certification more clear? I don't think you need a set of limited standards? I

wouldn't suggest that the standards ought to be limited.

We have certain functional requirements that we believe need to be met. A system that meets them gets certified and a system that doesn't, doesn't. That is my view of it.

>> KING: Thank you, Pete.

>> RYAN: I will have a try and make some comments. The more I hear, the more I am glad I didn't try to lead on this. Because I realize there are all kinds of hidden agendas and things which I didn't appreciate at the outset.

Well, let me speak to the first question, how do you evaluate these individual systems? Strikes me that that's profoundly difficult problem. I think it goes back to the discussion we were having this morning about how do you set up your threat models and so on and so forth.

So I think I would just suggest -- that

strikes me as a very difficult one. I don't know if you are expecting a real answer. The only thing that comes to my mind is that actually is going to require a substantial amount of research to come up with systematic ways in developing threat models, which will -- in a sense, it comes back to your question earlier.

I think the threat models and so forth are dependent on the systems. If you come up with completely new kinds of technologies, you introduce totally new classes of threat and so forth. So I think this is a profoundly difficult problem, will be my first comment.

Yes, I think I'll leave it for that. And hand it over to someone else for a minute.

>> KING: I'll respond. I think that is -- it is a challenge, as we're trying to, if you will, kind of wrap our minds around the risk assessment threat assessment models, for lack of a better term, for conventional systems moving through the VVSG process, what will be the threshold of uniqueness in an innovation system that will require the research of a

different set of models perhaps to validate it.

So from -- from my perspective, as I'm looking at -- not just the current VVSG but the past and future ones -- is trying to understand the overhead that is embedded into the application of the VVSG and how that plays out in terms of time-to-market decisions, cost-to-market decisions, and cost to the jurisdiction.

And the one thing that we know is that they're always unintended consequences, so trying to think through concurrently, not only the rigger of the proposed VVSG, but also the implications of the innovation class model, I think, has added a level of complexity, at least in my own analysis.

John first, and then Costis.

>> WACK: I thought I would just talk a little bit about what is in the VVSG, and as best I understand it, why it turned out the way it was.

At a certain point, in writing requirements for new systems, there was a decision made by members of the TGDC that we couldn't write requirements that were specific

enough, good enough, for some emerging technologies, such as cryptographic systems, so there was a desire since these systems, in essence, looked good, to somehow or the other create a pathway to getting them certified, even though there aren't currently requirements in the VVSG.

So that's how the innovation class came about. And then people struggled for a long time about, okay, how do we still write specific requirements for taking systems that we don't have specific requirements for and get them through the certification process?

And eventually people started to look at it as a standards maintenance issue, which means we've got a problem here, and that is, how do we update the VVSG in a sense so that it -- new requirements for new types of systems can be added to it? And what can we write currently that is specific, that labs, again, can use? Because labs need very specific

requirements that they can test to. So the innovation class was born in a sense.

And to a large degree, a lot of those questions up there are really directed toward

how can the E.A.C. do this? Because the VVSG doesn't report to do this. The VVSG has some requirements in there that essentially say innovative systems should meet all of the other requirements in the VVSG.

But the E.A.C., in a sense, was tasked by the TGDC -- or was recommended by the TGDC to come up with a system for actually looking at these new technologies and figuring out how to get them certified and tested.

So, to a certain extent, I think it is -- I hate to put it this way, but it is the E.A.C.'s problem, at least that is the way the TGDC kind of drafted the VVSG. And they do need help. It is a very difficult problem.

I think we all felt that how could we actually do this within the constraints of a standard and felt that we could not, that it

19 had to be a separate process from the standard
20 that might feedback into it at some point.
21 >> KING: Thank you.
22 Costis.
23 >> TOREGUS: Two or three thoughts here.
24 First of all, I have to agree with my colleague
25 to the left, that if the VVSG was, indeed,

1 performance based, we wouldn't need a
2 subordinate limited standard group.
3 And, in fact, from the discussion that we
4 had last week at the IPI roundtable on this
5 very topic, the question was raised about a
6 600-page document. And in my mind, performance
7 standards, you don't need 600 pages to describe
8 performance standards. You can describe them
9 fairly adequately in a small number pages and
10 then challenge innovation to occur.
11 Some people would almost have you think
12 that innovation and certification are an
13 oxymoron put together, that innovation somehow
14 goes beyond traditional certification, and then

certification catches up to it, and you certainly don't want to slow down that process of innovation.

But given that you've got an innovation class out there, I just wanted to put the other side of the coin.

In my own state of Maryland, we have a $1.6 billion budget deficit coming up. In my own County of Montgomery, we have $400 million of a budget deficit.

If somebody even understood there is talk

about changing the machines we use for voting to get it one more time, I think people would just freeze. They just wouldn't be able to rationalize it.

So instead of an innovation class, maybe we also ought to think about some kind of a, let's say, transformation class.

Given the machines that we have today, what is it that we can do to the systems or on the machines, the software inside the machines, so in fact, when they become more parallel to

what the VVSG would have us think.

I think the notion that we're designing from scratch systems has to be balanced with the notion of where are we budgetarily in the states and in the counties. We can't just say we imagine a new system to come into play, especially since we just had a new system come into play.

So in addition to the innovative systems, I would like to put in a good word for how do we transfer the existing systems we have to become VVSG compliant so in some kind of transformative systems, rather than only innovation systems. It might be an idea that

we could have some fun talking about.

>> KING: Okay. Juan?

>> GILBERT: In the innovation class, it talks about -- well, one of the things that I think is important is when you submit for the innovation class -- I guess no one has done this, so I am assuming you have to submit

material stating why you're innovative.

What is important to me is who is going to review that. It goes back to what I said earlier, about this balance of usability and security.

I think it is critical that whoever is reviewing innovation, it has to be a diverse board or a review committee. You can't have all security people on that committee making decisions because they like a certain technology that is secure to them, and then no one in the world can use it without a college degree in mathematics.

So I think it is important that -- I like the idea of this innovation class, and I think certain things, if we're going to have an innovation class and certify a system, we may, going back to what he was talking about, is

maybe certify aspects or methods or components of systems that could be integrated.

So if you're going to -- for example, a multi-modal interface, there is clear

usability, performance benchmarks in the VVSG.

If you can meet those, then could you potentially certify that as an innovation, because it is clearly something that is innovative that could be attached to existing systems, or do you have to certify the whole system?

And that -- I don't know the answer to that, but I am throwing it out there, is that do you provide component certification, or is there a whole system?

In either case, I think it has to be carefully decided on who that review committee is composed of and their backgrounds such that we get an optimal decision.

>> KING: Okay. Thank you.

Brian?

>> HANCOCK: Thanks, Merle. I want to piggyback what Costis said and what Juan was talking about.

You know, there are a lots of things we

don't know about what is going to happen with the next iteration of the VVSG, but I think there is a couple of things that we certainly do know and I think probably all of us here can agree on. Looking at the document as it is, I think there are things that everyone needs to be aware of, especially our policy makers, legislators and people that are going to be making decisions at that level.

First of all, whatever this comes out looking like, the testing is going to be exponentially more expensive than it is currently. I don't think there is any way around that, given the way it is right now. Second of all, pretty obvious that no system out there, and I would include Op Scan systems could meet this document as it is currently written. Those are two things that we know and I think we need to throw out there for everybody to think about. Okay. Daniel.

>> CASTRO: I just wanted to expound a little bit on what Juan said. I think that is a very important point because innovations have historically been good for voting systems and voting technology, but the idea is that

innovations can be small and large and can be very incremental. But the cumulative effect often that is what we are really after sometimes.

It is not clear from the current innovation class standard which I think the idea of an innovation class is good in the sense that it recognizing, that the VVSG is recognizing the importance of innovation but bad in the execution of it.

But I don't think it gives a clear path to certification, especially for small innovations. You may have a very small innovation and a lot of people question, is it worth going through a very complicated innovation class certification process? But that small innovation may still be very useful. It may be a minor cost savings, but these many minor cost savings would add up.

The second point I want to make is that -- I think we talked about this a little bit -- is that the innovation class is currently defined as really a subcomponent of software independence. That is the other method or

25 means by which a vendor can get software

1 independence. But again, when we talk about
2 functional standards versus design standards,
3 like I have said before, I think software
4 independence is really design standard. If you
5 want to have true innovation, you have to make
6 innovation class purely functional. It should
7 be outside of any kind of design standard. In
8 this case, it should be outside of the software
9 independence class.
10 >> KING: I have a comment that really
11 tries to tie together three different groups of
12 people who are indirectly mentioned in both the
13 conversation today but also in the VVSG.
14 I kind of put this under the heading of
15 the unintended consequence. And it is the
16 individuals involved in open-ended
17 vulnerability test, the individuals involved in
18 reviewing innovation class proposals, and the
19 individuals involved in risk assessment of
20 systems. And what is implied is that there

will be individuals who possess some skill and some knowledge and perhaps some experience for that. But I think what we have heard from Juan and heard whoever made the comment on the OEVT that the success of those components of the

VVSG will be in large part dependent upon the abilities and skill sets of those people. And I am not proposing that that be something that we resolve here today.

But I pointed out as for most of us who are involved in managing organizations, staffing is the absolute hardest thing that we do, identifying people who have the skill sets, the time, and the availability. And so when I read through the VVSG that is one of things that struck me is who are these people? Where do we find them? How do we train them? How do we certify them? How do we supervise them? How do we evaluate them? And again under that heading of unintended consequence, that would be instructive to better understand in terms of assessing the doability of the innovation class

and also the open-ended vulnerability testing.

>> GILBERT: Yeah, we need a functional spec for the selection of the individuals.

>> KING: Well, I bring it up because the intersection of people who understand voting systems and security, etcetera, it is still a relatively small number of people. And I think we need to pay attention to not only the

unfunded mandates but in this case almost the human resource mandate that is imbedded into the VVSG. John.

>> WACK: Well, I will not be working in this forever and I do need a job after this one. Probably the rest of us we could form a corporation here. But I agree completely with you. And at the same time though I do have to mention that right now NIST has this national voluntary laboratory system program and part of that program really is about making sure that labs, whatever they test, have individuals with sufficient knowledge and experience and things

of that sort.

I could see that the criteria for voting system labs will need to be updated somewhat. There will probably have to be more work done with that particular program to make sure that the right level of experience does get in there.

>> KING: Sorry. Ron.

>> RIVEST: A couple of things with regard to innovation. I think one thing that hasn't been said and maybe is just obvious is the importance of supporting innovation in this

area. It is an area where we all realize that we are still not where we want to be with voting systems. I think academics are realizing that the voting systems are an interesting problem area to work in.

We are seeing more and more academics trying to put their students to working, trying to come up with better voting systems and improve it. We are seeing innovation in part because of the attention getting and also

because it is a hard problem. Voting is really one of very toughest problems I have ever seen in the security area. The requirements are contradictory. People get challenged by that.

So we are seeing people come out of academia or out of the wood work, whatever, and working on this as you might not otherwise expect. So innovation is happening in this area. The question is how to integrate that into the certification process.

Juan said something I would like to support as well. Is it something on the TGDC we were not able to do is which was to support certification components of voting systems. And I think that has the potential, it is a

hard issue how do that well, but trying to support certification of the components could open the door to a lot of interesting innovation. If you have an Op Scan system which was just the scanner part and couldn't talk through a standardized protocol to a

tabulation system in itself was a separately certified piece and interfaced standards that were supported, I think it would open a door to a lot more innovation. But I think we are a ways from that kind of vision yet and making component certification work.

I think when we are doing new things, and I think some of the cryptographic systems are very interesting new proposals, and how to think about certification. I think what John is saying is right, too.

We can have a more open process, a somewhat higher standard kind of thing. You can make it more public and might even require source code to be public or do other things, have a lot of public hearings on innovative ideas, so that it is a different kind of process in a more transparent way. And this may help increase confidence. You're not

getting unintended consequences, as Merle is concerned about. That's it.

>> KING: Juan?

>> GILBERT: I would just like to make a comment about this, going back to something Merle said a while ago in some meeting we had.

When you think about what we're doing, we're talking about election science, and there is really no discipline -- can anybody go and major in election science?

I mean, how do you learn how do this kind of stuff? So from my perspective, and Merle knows I always go on the bandwagon about this, we're talking about election science, and it is not rocket science. It is harder.

At least rocket science is a defined field. At least you can get training in it. At least there is something there.

Here, what do we have? We have disciplines that have traditionally been in silos, you know, separate disciplines that are coming together trying to do something that has never been done before, and we really don't have true training on how to do this. So we're kind of making it up as we go along in one

sense, but I think we are kind of hard on ourselves, too.

So I think the VVSG -- and maybe this could have been a summary -- but I think the VVSG is a step in the right direction, and we're definitely critical of it.

But, again, keep in mind that there really isn't a discipline or a book for dummies on how to do this stuff, so...

>> KING: Juan makes a good point. I just saw where NASA has postponed the shuttle launch for a month because of a failed fuel cell sensor.

And if we have bad fuel cell sensors on our election equipment, we are still going to have an election on election day, so maybe it is a lot more difficult than rocket science.

Peter?

>> RYAN: Yes, a comment that Ron just made that prompted in my mind, that moving to, say, cryptographic systems, that potentially changes the certification game, because it almost then becomes a much more public process.

It's much more transparent. What you are trying to evaluate there are the

crypto-algorithms, the protocols, and I guess, to some extent, the procedures around them and so forth, rather than trying to certify a lump of code.

And that is, in a sense, precisely the point of making the thing software independent, is that it doesn't depend on certifying a lump of code. So in some sense, you're changing the certification game there, and potentially making it perhaps easier and cheaper, perhaps.

Just to come back, you made some comment, I think, that the innovation class is likely to make things exponentially more expensive to certify, or something to that effect.

>> Just the VVSG [indiscernible]

>> KING: Okay. Alec?

>> YASINSAC: I think one of the things we haven't really addressed. Peter, you just raised a perfect issue. And while it may be more transparent in terms of everything is out there in the open, I think what it would mean is very, very far fewer people would be able to have any real idea of what was going on.

24 I mean, if you look at the number of

25 programmers there are in this country that

1 really understand how to write C plus plus,

2 that is a small percentage of the population,

3 but if you look at the percentage of people who

4 could understand most of these algorithms, it

5 is extremely narrow and extremely small, which

6 is one of the large challenges of that

7 solution -- of those set of solutions, I should

8 say.

9 >> KING: Ron?

10 >> RIVEST: I would like to respond to

11 that issue. It is one that is raised often

12 with cryptographic systems. And cryptography

13 is the use of mathematics for integrity and

14 secrecy. It is a technology that has been

15 around for quite a while. It's taught at lots

16 of universities.

17 And in some ways, it's much simpler than

18 software. So if your choice is understanding a

19 few equations and understanding 10,000 pages of

code, you know, I think the choice is clear as to which one is more digestible. In fact, the code isn't even available to look at here.

So I think it is a bit of a false issue here. When you think about how people develop confidence in systems. Some understand it

themselves, and I think ones that are publicly documented with technical articles that you can read and digest that will be popularized for this stuff, too, will