TECHNICAL GUIDELINES DEVELOPMENT COMMITTEE

(TGDC) MEETING

Monday, December 4, 2006

Greene Auditorium

NIST Gaithersburg, Maryland

(**START OF AUDIOTAPE 1, SIDE A**)

DR. WILLIAM JEFFREY: Good morning. If everyone could take their seats. We'll be starting in just a minute.

Welcome, I'm Dr. William Jeffrey, the Director of NIST and the Chair of the Technical Guidelines Development Committee. I hereby call to order the seventh plenary session of this committee.

I would like to begin if everyone could please stand for the Pledge of Allegiance.

At this time I will recognize Mr. Phil GREENE, again, NIST General Counsel and request that he determine whether or not a quorum of this committee is present.

MR. PHILLIP GREENE: I will begin with a roll call. Williams.

MR. WILLIAMS: Here.

MR. GREENE: Williams is here. Berger.

MR. BERGER: Here.

MR. GREENE: Berger is here. Wagner.
MR. WAGNER: Here.
MR. GREENE: Wagner is here. P. Miller.
MS. P. MILLER: Here.
MR. GREENE: P. Miller is here. Gale. Gale? Mason.
MS. MASON: Here.
MR. GREENE: Mason is here. Gannon.
MR. GANNON: Here.
MR. GREENE: Gannon is here. Pearce. Pearce? Pearce is not responding. A. Miller. A. Miller?
MS. A. MILLER: Here.
MR. GREENE: A. Miller is here. Purcell.
MS. PURCELL: Here.
MR. GREENE: Purcell is here. Quesenbery.
MS. QUESENBERY: Here.
MR. GREENE: Quesenbery is here. Rivest.
MR. RIVEST: Here.
MR. GREENE: Rivest is here. Schutzer.
MR. SCHUTZER: Here.
MR. GREENE: Schutzer is here. Turner-Buie.
MS. TURNER-BUIE: Here.

MR. GREENE: Turner-Buie is here. Jeffrey.

DR. JEFFREY: Here.

MR. GREENE: Jeffrey is here. We have thirteen in attendance. That is a quorum.

DR. JEFFREY: Thank you Phil. I would also like to thank you for the service to the TGDC. For those who don't know Phil has gotten an excellent opportunity to spend a year overseas and we are going to miss you. So, thank you very much.

I would also pleased to welcome four new members to the TGDC, Ms. Tricia Mason, Philip Pearce representing the U.S. Access Board, Dr. David Wagner representing the American National Standards Institute, and Mr. Paul Miller representing the National Association of State Election Directors. I am going to invite each of these members to give introductory remarks if the would like and I will start with Tricia, if you would like to make any statements.

MS. MASON: I'm going to get the microphone. Can you hear? Have I got it hooked up right?

Thank you, I'm Tricia Mason, representing the United States Access Board. I look forward to working with this committee as well as the Election Assistance Commission's

Board of Advisors and it should be a very interesting meeting. I look forward to all of the comments that everyone has and I look forward to working with all of the other Board members. Thank you.

DR. JEFFREY: Philip Pearce.

FEMALE SPEAKER 1: No here.

DR. JEFFREY: Not here, sorry. David, would you like to say anything?

MR. WAGNER: Well, thank you. It's a pleasure to be here and to represent ANSI and I thought I should mention up front that consistent with ANSI's policies, I'll be abstaining on all votes. I'm looking forward to working with you and I hope you – please don't take that as a rejection or endorsement of anything that folks are saying here. I just wanted to get that on the table for starters. Thank you again.

DR. JEFFREY: Paul Miller would you like to say a few words?

MR. MILLER: I'm Paul Miller and I'm representing NASED which is the organization that sort of got this whole process rolling and filling the shoes of Paul Craft who has been part of this process from the very beginning. They

are huge shoes to fill but I'm looking forward to the challenge. Thank you.

DR. JEFFREY: I would also like to offer if any other member would like to say something, Steve you wanted to say a few words and anybody else after.

MR. BERGER: Thank you. Late last week there were three draft resolutions that were circulated and we will be considering these later in the meeting. I believe tomorrow. I wanted to just give a couple of words of introduction to explain the intent behind them.

In the Core Requirements Committee we have had a number of discussions focused at how we best tie or efforts into achieve maximum effect in the voting system. The three resolutions that are out there are basically looking to further that exploration and make sure that our efforts are as directly linked to the problems we are seeing in the field as possible.

Let me just introduce them by saying the first one is primarily looking at the issue of the causal factors that created the system as we have it today assuming that that system was created with good intent and for rational reasons. Basically it asks what are the trade offs that we are looking

at.

The second resolution is asking to survey the recent experience in the last two elections and map what we are doing to those issues that have arisen in the field.

The third one asks a fairly simple question but an important one and that is, what problems are best solved by revisions to the standard as opposed to changes in other points of the system.

So, with that I'll leave it and we can take them up later.

DR. JEFFREY: Okay. I would like to acknowledge that Mr. Philip Pearce of the Access Board has joined us and if you would like to say a word or two of introduction feel free.

MR. PEARCE: Thank you very much. I'm sorry I'm a little bit late. We ran into a little bit of a snag with the transportation but I think we got it all worked out.

I appreciate the opportunity to be here and to work with this group. I've tried to bring myself up to date and one of the things that I have found is that you guys have written a lot of stuff and its good stuff and I appreciate the hard work that you've done and I look forward to getting

a chance to work with you and to, hopefully, provide some insight from my perspective on that. So, thank you.

DR. JEFFREY: Any other comments from any members? Okay.

Nebraska Secretary of State John Gale and Ms. Sharon Turner Buie, Director of Elections for Kansas City, Missouri will not be able to attend today due to current responsibilities in certifying the November elections. They will join us via teleconference as the schedules permit.

I would also like to acknowledge and thank four departing members of the TGDC, Dr. J.R. Harding, Mr. James Eleckes, Mr. Paul Craft and Mr. David Karmol who has served this committee admirably and we are a lot better off for the contributions that they have made. So, thank you very much.

The committee is pleased to have U.S. Election Assistance Commissioner Donetta Davidson in attendance and some of the senior staff from the EAC and we will be receiving comments from her shortly. I look forward to her comments regarding the work on this committee.

First, I would like to entertain a motion to adopt the TGDC meeting agenda. Is there a motion to adopt the agenda?

FEMALE SPEAKER 2: So moved.

DR. JEFFREY: Okay, a second?

MALE SPEAKER 1: Second.

DR. JEFFREY: So there has been a motion and a second to adopt the TGDC agenda. At this point do I just ask if there is a unanimous consent or do you? I'll have to check with the Parliamentarian on these things? Is there – to adopt by unanimous consent the agenda? Any objections? Not. So moved.

Okay, at this time I would also like to entertain a motion to accept the minutes of the March 29th meeting of the Technical Guidelines Development Committee. Is there a motion to adopt the minutes?

MALE SPEAKER 2: So moved.

DR. JEFFREY: Okay, is there a second?

MALE SPEAKER 3: Second.

DR. JEFFREY: Okay. If there is no objection I move for a unanimous consent on the minutes. Any objections? So moved. The minutes are accepted.

For those in the audience and those on the webcast who are new just let me give you a quick review of who we are and why we are here.

As a brief review, lets start with the Help America Vote Act, HAVA, which established the Technical Guidelines Development Committee. HAVA charters the members of this committee to assist the Election Assistance Commission with the development of voluntary voting system guidelines. Since the last meeting of the TGDC, three working subcommittees have continued drafting and editing preliminary reports on issues pertinent to voluntary voting standard recommendations in the areas of human factors and privacy, security and transparency, and core requirements and testing of voting systems. We will be discussing these reports today.

Recent news reports regarding the vulnerabilities of electronic voting systems contained in one of the reports to be discussed today have raised the question of whether the report's recommendations represent the official position of NIST. This draft report was prepared by staff at NIST working with the Security and Transparency Subcommittee at the request of the TGDC specifically to serve as a point of discussion at today's meeting.

The report is a discussion draft and does not represent a consensus view or recommendation from either NIST or the TGDC. The TGDC, after discussion today, may adopt, reject

or modify the recommendations.

Those adopted by the TGDC will be developed into guidelines that will be presented to the Election Assistance Commission for consideration. Any draft guidelines approved by the EAC will undergo stringent review, including public comment before they are issued as final guidelines.

Now, we have a lot on today's agenda and so the time required to accomplish these items means that the committee cannot take public comments at this meeting. Comments and position statements regarding the work of this committee should be sent to Voting@NIST.gov where there they will be posted on the voting website. Comments we have received to date have been posted and reviewed by NIST staff and TGDC committee members.

At this time I would like to invite EAC Commissioner Donetta Davidson to address this committee. So, welcome Commissioner Davidson.

MALE SPEAKER 3: If I may make just one comment. If anyone needs the services of signers we have them over stage left. Please come down to the front. They will be here during the whole meeting. I'll make this announcement later, again. Thank you.

DR. JEFFREY: My apologies. I forgot to also mention terms of safety. If there should be an emergency, there are four exits clearly marked. We do not anticipate an emergency, but if so, please exit in a controlled fashion and follow -- there it is. Thank you. So, with that, Donetta Davidson.

MS. DAVIDSON: Thank you. Good morning. Thank you Dr. Jeffrey and the TGDC committee. We definitely appreciate all your hard work and thanks for having me here today.

We are today discussing the future of the voting systems and to make sure that the guidelines that you produced and we produced keep up with the pace of technology and at the same time be secure, be accurate and reliable. That's a tall order but I am sure that we can all accomplish this as we work through it. As I said, I do thank each and every one of you for what we are doing.

The first thing I would like to go through is the time implementations that we are dealing with currently because I think its important as we move forward with everything that we are doing that we take into consideration the time element. As you can see up on the slider of what you have in front of you, we passed the VVSG 12/13/05. That will

be implemented and have to be in place on 1/1/07. The EAC implementation of the voting system testing certification take effect 1/1/07. We have just gotten through our public presentation of it. It will be adopted at our meeting this coming Thursday. So, our testing certification is up and will be running at that time.

We will be testing to both the 2002 VSS and the 2005 VVSG. All systems have to come in and be tested to those. We are starting the process so all the manufacturers have to bring their equipment in and be tested after the January date. All systems will be tested to the 2005 only requirements after 12/13 of '07. We will not test at the 2002 after that time frame in 2007.

The TGDC and NIST will forward a draft of the VVSG, the new iteration to the EAC July 31, 2007. That's the date we have pretty well put into play. The EAC at that time has to go out for public hearing, comment, meet with the standards board, the board of advisors and then they will, it is also in the Register for ninety days and we will take comments. The last time we received over 6,500 comments. The time of really working through that process it does take a great deal of time. So we anticipate that we will

adopt any time from the end of November of 2007 into the Spring of 2008. So, what you are working on now will not be adopted until that time. I think its important that you realize how much time it does take to really get it accomplished after its delivered to us in July.

In moving forward, I would like to take a moment to examine all of the options that we have before us. As being involved with elections a great deal of time and as a former Secretary of State, I can tell you firsthand that one size does not fit all. We need to remember that there is different laws in every state. That there is different requirements that they have to meet within that state. There are time factors that definitely flow into that also.

We have to take account when we are looking at the new technology to make sure that it works into the needs of all states. I believe the VVPAT is only one option. We should continue to research other forms of verification because technology and solutions in this area, I believe, is rapidly increasing.

I think there is one issue I would like to tell you about and it hasn’t happened yet. We know the courts are above all of us. They are the ones that make the decisions

at the end. If there is a recount that is held in some state because of a very close election and it goes to the courts and they had a VVPAT and in that VVPAT, because of it either not being inserted, the paper not being inserted correctly or it jammed or the printer some way or another failed, what's the court going to do and decide when the number of people that appeared at that poling place is different than what is the recorded number of paper that was recorded. The machine has that number on it but the paper is missing. What's a judge going to do in deciding that? There's two official ballots or is there one? Some of the states have said the paper is but is a court going to disenfranchise those people that showed up at the polling location to vote and their vote is not being counted because of an error of a printer? That is why I really say we need to keep our doors open to technology. If we were there and it worked perfectly, I wouldn't say it at all. Any time we can improve the process in elections we need to keep that open and not close the doors.

We cannot also forget that HAVA instructs us to make sure that the people with disabilities are able to vote private and independently. I believe that we have to consider

their rights as we move forward.

The last thing that I would really like to do is give you a little bit of an agency update. Usually Tom Wilkey does that but he is with an ailing relative right now and can't be with us.

Its been a busy year as all of you know, for the states, for the locals, they have been putting in to their plans not only the state laws changing within their areas, but they have had to meet two HAVA deadlines. A voter registration system and also they had to meet the new equipment. We had over thirty percent of our voters voting on new equipment this last election. You know what, the election officials, poll workers, voters had a very successful election. They met the challenge.

Election day went a lot smoother than people anticipated it would. According to the public and the media reports we have over 6,700 jurisdictions that ran elections and only 39 reported problems. That's less than one percent. Most of our officials have contingency plans in place, extra paper ballots, back up batteries. They extended polling hours in some places.

Election officials, poll workers and voters

successfully met the challenge of election day. The exit polls that were done by CNN even showed that 88 percent of the voters were confident that their votes were counted accurately and the election was being handled very securely.

As we move forward we are continuing to see how many of our states have met the HAVA requirements under Section 102 funding to make sure that the new equipment was actually out there. If it wasn't then the money has to be replaced back into the fund so it can be delivered back to the states. We are reviewing and working on that with a great deal of effort.

As the last thing I would like to say is, I do appreciate the work that each one of you are doing here on this committee. It is very important and I would say this probably is one of the most important meeting that the TGDC has in place today and tomorrow than they have ever had before because you are developing a new system for the future. I mean the future. We won't be doing this every time we turn around. This is the future. The manufacturers have to have time to develop and we have to have time to implement. That's why I really talked about the time frame because as you move forward, obviously I hope time frames is one of the things

you discuss.

Thank you very much.

DR. JEFFREY: Thank you very much Commissioner Davidson. We very much appreciate those words.

With that I would like to ask Mr. Mark Skall to come and to provide a summary of activities since March 2006. So, Mark.

If I could also mention to the members that there are copies of the view graphs contained at the very front of the binder.

MR. SKALL: Thank you. I would like to give you a summary of the activities that NIST has been working on since the last TGDC meeting.

First of all we have been very, very busy doing research leading to the eventual development of the VVSG 2007. As you know we work very closely with the subcommittees in doing this research and, of course, the TGDC itself makes the final decisions as to what goes in the VVSG 2007.

Secondly, we've spent a lot of time trying to improve the access and coordination with the TGDC. We have done other activities relating to coordination with other bodies, other research and we have had some interactions with

Congress as well.

What you see in front of you is a fairly detailed list of some of the main issues and research that we have been conducting in the human factors and privacy subcommittee. We have worked on usability, performance benchmarks and usability requirements, accessibility requirements, core requirements and testing committee. We have a lot of contentious issues we have been looking at and researching., the Cox exemption, mean time between failure standard, reliability, accuracy, coding conventions, quality issues.

In the security and transparency committee, of course we have done a lot of research on software independence, DRE security issues, software IV, end-to-end cryptographic systems, VVPAT wireless and set up invalidation as well as many of the more traditional security areas that will be incorporated into the standard once its agreed upon by the TGDC access control crypto set up validation, etc.

I just wanted to say a few words about coordination with the TGDC. We've revamped our TGDC website which we believed has improved usability and navigation including project management information. We've included a resolution tracking matrix that the TGDC has asked to produce which

shows the relationship between the resolutions and the work we have been doing.

Since the last TGDC meeting there have been 47 tele-cons. There has been a lot of communication, a lot of work. We've prepared discussion papers, draft material. There have been numerous individual discussion. There has been one face-to-face meeting. The security committee has met in Boston. I want to thank all the TGDC members and NIST people for attending that. I believe that was over the weekend. So, there is a lot of extra work that clearly has gone into this effort.

We have on our website the outline of the VVSG 2007. There is a new format we are proposing and we have in there a draft so we have the stable material in there and issues are debated by both the subcommittee and the TGDC planning, we then can include new material in there and eventually build the VVSG 2007.

We've had a lot of meetings. We meet monthly with the EAC. We have a very, very close coordination with the EAC. In fact Commissioner Davidson and I speak probably almost daily. Clearly we work hand in hand in what NIST and the EAC and the TGDC are trying to accomplish.

One of the things that we've really tried to do for this particular version of the guideline is to do a lot of outreach. In the first version, the 2005 VVSG, we were constrained by the nine month time limit given to us by HAVA. We didn't have as much time to go out and speak to as many people as we would like.

For this particular version, we wanted to reach out both to voting system vendors as well as election officials. So, we have monthly meetings with the vendors through the ITAA, Information Technology Association of America. We try to liaise with as many voting officials as possible and we do speak to one from the AC Standards Board as well as others.

We meet and coordinate our work with other researchers. We have given many presentations and visits with election officials. We have also observed and volunteered at elections.

Dr. Jeffrey testified before the House of Representatives committee on, there was a joint hearing of the House Administration and the Committee on Science. I and a few EAC commissioners, Commissioner Davidson and Commissioner Hillman spoke at a voting town meeting hosted

by Congresswoman Melinda McDonald who at the time was the ranking member of the House Administration Committee and is now the chairperson.

Again, we have posted on our website the resolution matrix that the TGDC asked us to produce. It's a fairly extensive matrix which shows the resolution and it shows which particular version of the guideline that it applies to, which subcommittee is working on it. So, there's a lot of information there that tracks the resolutions.

I would like to speak a minute or so on the meeting agenda. As Commissioner Davidson said, this is an incredibly important meeting with many, many key issues to be resolved. We have three hours to discuss the STST issues, three hours to discuss the CRT key issues and we have given two hours to human factors. We think those are probably just a little less contentious. We can, of course, adjust the schedule if this doesn't work out.

We have also reserved two hours for resolutions tomorrow. Resolutions can be made at any time. The reason we really reserved more time than usual for resolutions on the second day is with all the key issues that will be discussed the first day, in case consensus can't be achieved on the first

day, often times at meetings like this, I think its helpful for people to take a deep breath, go out to dinner, have a drink or two or three or four and perhaps look at the things and perhaps arrive at compromises and draft precise wording. So, we reserved a lot of time tomorrow if that needs to happen.

Strategies for today's presentations by the NIST people. Let me give some brief high level summaries. I think in the past we've perhaps spent a little too much time summarizing all the material. We produced all of the material. We assume everyone has had a chance to read it and we are going to give high level summaries to most of the material and spend most of our time on the key issues. We want to spend time debating the ones that people feel strongly about.

So we are going to give presentations today for each of the three committee work. I would just like to also preface this by saying that the subcommittees try very hard to arrive at some sort of consensus and provide recommendations at these meetings. Sometimes they can. Sometimes they can't in between the plenary sessions. I think the security and transparency committee and HFT essentially have arrived at recommendations which you will hear today.

Core requirements and testing hasn't achieved a consensus on most of the issues. So, the presentations today that we will be making for core requirements and testing, we'll just try to give a description of the issues without presenting any consensus from the subcommittee.

So, today right after these presentations we will begin the security and transparency committee presentations followed by core requirements. Core requirements will continue tomorrow and human factors and privacy will conclude the plenary.

Any questions? Thank you.

DR. JEFFREY: Thank you Mark. At this time I would like to invite Mr. John Wack to present an overview of the planned VVSG 2007 document structure.

MR. WACK: Okay. Good morning. Welcome to the new members and its always an honor to be able to address you. What I'm going to do is just take up five minutes of your time. Very quickly I am going to give you an overview of the document and where we are and talk about some things that may not be entirely obvious to you but its part of our job here. If I can work this correctly.

Okay. Basically at a high level I am just going to

talk about some aspects of the document that make a big difference in the quality overall and how well it will work out for our customers. Who our audience is, some issues we are addressing with regard to format usability. We are trying to do things to facilitate your review. I will give you some high level status. We will talk a little bit about the months ahead which should be interesting.

The first thing I want to get across is that we have two jobs here at NIST and one is to write requirements. One is to do a lot of research and come up with good requirements. The second thing, I think, which is almost equally as difficult is to put it together in a document and make it understandable. Along the way we have come to recognize that not only are the quality of the requirements important, but also how well people can understand it. That in itself is an art, you know, just basically putting this together in a way that everybody can find the material they need and understand it correctly.

So, we have a difficult job because we really have to write for vendors and test labs and states. Basically they have to be able to find requirements they need, interpret them unambiguously and make decisions based on them. We

first need to write for you as well. We need to get you to be able to understand the material. We need to be able to write for the public.

This document has to go out for a public review. There will be many different audiences judging it at that point. So, we recognize that the better job we do getting across our material, the better job you can do in judging it and the better job the public can do in assessing it, whether its right or not.

What we are attempting to do is deliver at the end of this exercise to the EAC a well structured, well formatted document, a highly usable document that they don't have to go through a lot of trouble with to reformat and put in shape for public review. Thus we are coordinating with them and we plan to give them something that basically works very well for them as well. It would just make sense to do that.

We are working – I would like to thank Whitney Quesenbery especially who has helped us out a good bit in ideas with regard to just simplicity, plain language, flattening the structure more and just make it easier to navigate.

What we have started to do fairly recently is assemble draft versions of the document and the format we've chosen,

I think we are up over 500 pages at this point. We are doing that for a number of reasons. One is just to see how well it hangs together. Another reason is to put all the material together at once and allow you to take a high level look at it and see how well it works together. There are many areas of the requirements that overlap. Core requirements overlaps with security. Security definitely overlaps with human factors.

This also gives you an opportunity to judge firsthand whether you find this format usable. So, any feedback there is of course very welcome.

Here is a reminder. You probably know this already but we have five volume we are producing. An introduction, a second volume that talks more about the glossary, volume three and four are really, I'd say the big chunks of the document. They have really the big requirements there, product requirements and volume four is data, standards on data to be delivered, vendor, test lab requirements. Volume five are test methods. They are to test themselves overviews of tests, overall methodologies.

So all volumes are under active development. We don't have volume one filled out with a lot of material but we

do have a lot of introductory material. As I said, we are, at this point, running over 500 pages. We want to produce something that works, not only in print, but works on the web. We need to come out of this meeting with a lot of decisions and good directions of where to go in the future.

So, I'll talk about the months ahead. We are going to be very busy. Not only do we have to build this overall document but we have to populate it with a lot of clear requirements. We are going to have to focus a lot on continued tele-cons and making material available. What we have been doing more of late is actually giving you small white papers and small discussion papers as opposed to just the material themselves, just the requirements themselves. We think this will facilitate your understanding of the material in your review.

By the next meeting, we haven't scheduled that yet, but we should have a very substantial amount of material for review. I wanted to say that we have basically seven months left though. I think last July I thought to myself oh, the TGDC meeting in December is a long way off and boom, its come upon us. I say seven months really because the

process of putting together a document is going to take some time. We will finish up. We will finally get your reviews. We'll know what to do and then we will have to assemble it. That will take a couple of weeks before we are ready to give it to the EAC.

With that, any questions I can entertain or we'll talk about this later? Okay, well, thank you very much.

DR. JEFFREY: Thank you very much, John. Okay. We are actually a little bit ahead of schedule and given that the next section is slated to be two and one-half hours, I'd suggest that we actually start on the next section and then take a break partway through that.

So, assuming no objections to that – I've actually got four names listed on the next section. Who's up first? I've got Curt Barker, Nelson Hastings, John Kelsey and John Wack to present the security and transparency subcommittee preliminary reports and issues for VVSG '07.

FEMALE SPEAKER 3: Our first speaker is (undecipherable). So, let me go and get him.

DR. JEFFREY: Okay. So much for me adjusting the schedule in real time.

MALE SPEAKER 4: There have been some questions

from a couple of folks. If you are listening on the webcast, this will be in archive format so you can listen now or later. Also the URL for all the people here is right off our main web page, vote.nist.gov. It's the second link down. All of the slides that you seek presented today will be available, probably tomorrow morning, again off the main webcast. So, we do make them available although we didn't make copies for all the public.

The other thing is, if we run out of materials, we are getting a little bit low and if you didn't get any hard copies, just leave a card out there and I'll get you a hard copy or you can also get those off the website as well.

As far as your name tags go, please keep them with you. If you are coming back tomorrow, it makes it much easier to get back on campus with a license. You don't have to go through the security trailer. Also please wear it throughout the building. This has been a very good audience because I haven't heard a cell phone go off. I appreciate people keeping their cell phones off.

To the committee I would just like to recommend to them we lost a very valuable member in Mr. Craft who always identified himself before he spoke. I still got some low

grades last time from people who didn't do that. Let me tell you why its important. The captioners – its easier for them to put your name up there and identify what you said if you just do that. It also helps the poor schmuck has to do the notes. Poor schmuck equals me. So, if you do that that would be great. I think we are ready.

DR. JEFFREY: Okay, so first up is Curt Barker. Again this is to start the presentations on the security and transparency subcommittee's preliminary reports and issues. Curt.

MR. BARKER: Thank you. I'm Curt Barker. I'm here to provide some introductory material for the Security and Transparency Subcommittee's Preliminary Reports and Issues for the VVSG 2007.

Our goals are to provide process integrity and maintain the accuracy of results in the voting system and as importantly maintain public confidence in the process, integrity and accuracy of those results. The public confidence has to be justified and founded on good rationale. We don't want public confidence and weak or broken processes because that doesn't tend to last very long. We are also trying for simplicity of processes for voting and election

officials and workers and of course affordability of the process and supporting mechanisms.

Security as we are treating it involves both features and assurances and audit trails are a key feature. We have to have assurance that unauthorized entities cannot add to, delete from or otherwise alter the audit logs.

We've looked at a number of different approaches to providing this process integrity and assurance and one of the things that we found is that a lot of the really interesting means for carrying this out would be easy to carry out were we not required to maintain secret ballots.

When you play secret ballot against the other assurance requirements we come up with a much more complex process particularly when we are trying for the affordability and ease of use.

When we look at process integrity perception is an issue as well. Any dependance on electronic instanciations (sic) of voter roles, votes and tabulated voting results offers the opportunity for questioning the integrity of the process. Its something that's harder to see, harder to touch. So, we need to come up with an overall process that allows us

to maintain our confidence in the integrity in an electronic environment or an electronically assisted environment.

One of the key issues is maintaining verifiable management of hardware and software configurations. For example, we want software that's been checked out to be the software that's actually employed in the voting systems.

Any input path to our processors that are capable of receiving information that can be interpreted as instructions or programming can be interpreted as posing a threat to the integrity of the process. So, we have come up with a number of mitigation approaches. Some of the things that might be done we can limit input capabilities such as interpretive input processing, single button input so that we limit the scope of what could be entered into the system. Limitation of input that are based on graphical user interfaces and then component to component channels that are inaccessible to the users.

Other integrity features that we have been looking at include cryptographic mechanisms to support source and content integrity and a number of non-cryptographic verification protocols.

What I have on the screen now are the preliminary report

contents. John Wack, the Information Technology Laboratory project manager who has been supporting the Security and Transparency Subcommittee will provide the details of those reports.

DR. JEFFREY: Thank you. Any questions on the introduction? John, you are up again. Thanks Curt.

MR. WACK: Okay. Thank you again. The presentation I am about to do is essentially a summary of certain STS recommendations to the TGDC as a whole. So, the recommendations I'll discuss have to do with what sorts of system ballot auditing capabilities the STS recommends for future voting systems in VVSG 2007. Professor Rivest is chair of the STS Subcommittee will follow me and he will discuss the concept that software independence which focuses on the ramifications and inadvisability of relying heavily on the correctness of the voting system software for the accuracy of the election.

He will also discuss recommendations for encouraging some new and innovative approaches that promise greater usability, assessability and reliability in voting systems.

John Kelsey of NIST will follow after that and among the topics he will discuss is NIST's experience with

attempting to draft requirements for all electronic voting systems but still don't rely on the correctness of the software for the correctness of the election results.

Lastly, I would like to mention to you that normally Bill Burr of the Computer Security Division would be doing this presentation. He is unable to make it here in person today and I would like to thank him for his very hard work and his leadership in this area. I hope I can present this to you as well as I know Bill would have done.

With that here are some more details about what's before us right now. I'll start with the issue of independent audits of electronic cast ballot records stored by voting systems and then I will move on to a discussion of the STS's work with independent verification. I will talk more about independent verification and what that means.

I'll discuss some issues with current paper based systems that implement independent verification and then lastly I'll discuss STS conclusions and recommendations. I would be happy to take your questions at that point but in the interest of time, I would prefer to introduce Professor Rivest at that point and then maybe take questions after that.

So, I've told you that we have seven months to go basically and we are at a major decision point in the development of our standards. We have to make a decision that will end up defining what types of voting systems will be permitted in the standard. So, we need to move past

(**END OF AUDIOTAPE 1, SIDE A)**

* * * * *

(START OF AUDIOTAPE 1, SIDE B)

So the conclusion is that VVSG 2007 should require voting systems that produce records of ballot choices that can be readily and independently audited. So, I will talk more on the sides ahead about what I mean by readily. Let us discuss first what we mean by independently audited.

Now there are many analogies that have been made. I'll make a quick one and that's basically the difference if you purchase something on-line versus purchasing it on the phone. Its just simply put if you purchase it on-line or if you purchase it in person, you do get a receipt. So that receipt serves as a record of your transaction. The bank also makes a record of it. The bank has its records. You have your own independent record. You verify the record. It goes along with what you think you bought. It is a verified record

and you can use that to make an independent audit of the bank's records. If you vote, I'm sorry. If you purchase something by phone you may not get that extra record. You may not be able to do at that point and independent audit of the bank's records. That may be fine. For STS we concluded that for future voting systems its better to have this independent record basically.

So, for example if you vote using an op-scan system. You filled out a ballot. You verified it for correctness. The ballot is then scanned by computer. It tallies up the votes. That ballot remains as an independent record of your choices and then later it can be used to independent audit whether the results of the election are right.

So why have we come to this conclusion. Maybe the first thing is that voting systems are computers that run software. Writing software is still an art in the year 2006. The larger and more complex the application, the more likely it is that there are going to be errors and for the application to behave in unpredictable ways that you can't basically test for.

David Flater later on is going to have a presentation on reliability and meantime between failure. He will make

some issues and points about how we are reaching a practical limit on our capabilities to test software to totally verify its correctness. When you add to the amount of software you have to test in a voting system, that there are other products in addition to that such as large operating systems, and these have a past record of requiring patches. Those have to be tested as well. So, testing is made even more difficult in many ways.

The direct record electronic or DRE voting system can be audited to a certain extent. You can check how many records its recorded, but its insufficient overall for detecting whether the ballot was recorded as cast by the voter. So the approach taken by the DRE requires relying on the correctness of its software to record the votes correctly. So its relying that the software was written well and that testing was thorough.

The computer science community has known for many years that writing software well and testing conclusively is a very difficult thing to do. We can expect that future voting systems are going to get even more complex in this regard. We are hoping they become more usable and we are hoping they become more accessible. So that’s a good thing, but

that means we will have more software to test. That is for sure. Professor Rivest is going to have to deal with the difficulties of testing more in his presentation.

One thing I want to focus on is how it is perhaps even more difficult to keep the software after its been tested working correctly after its out in the field. That's after its been purchased and used in elections in states.

Voting systems do get updated. As you know, sometimes quite often and it can be the case that updates affect other areas of the system and cause problems. Hopefully these updates are tested well, but it makes trusting the accuracy of the software more complicated and the fact of the matter is not everybody uses the latest well-tested versions of voting systems. We have many different versions of the systems out there.

So, its been my experience in the industry that many times when people get an application working correctly and they have it up, they do their best not to have to patch it. They want to leave it alone because it works. If they can get away without patching it, they do. If they do decide to patch it, it has to be done extremely carefully. They have back-ups ready. They are able to revert back to their

original version. Basically this adds to the complexity of trusting software and making sure that we have it tested correctly. So STS has concluded that it is a much more realistic and doable and simple thing to build in an independent audit capability.

An independent audit capability moves you away from having to trust exclusively that the code is correct. Engineers basically do this if they have the opportunity to. That is to design a system to be audited. The auditing capability in essence gives you much more confidence that the code is correct. You really want the code to be correct. The auditing capability gives you that confidence as well as testing.

Importantly, the auditing capability has to be used. If its complicated to use, it won't get tested. I should say that when we talk about security, we have to assume that we are also talking about usability. If its not usable, its not secure. So its no use having an auditing capability that presents lots of challenges.

I'm getting back to the word I used earlier. Readily. The auditing capability has to be designed to be used readily. It cannot make life difficult for election officials.

They have a difficult enough life already. So the auditing capability has to improve their lives.

So, we see two roads ahead of us in our goal to get a safe, secure and open and accessible elections. One route is trusting the accuracy of election results by trying to test the software and keep it correct and safe as it is fielded.

The other route is trusting the accuracy of election results by building in an independent audit capability and then using it after each election.

Okay, now you members who have been here for a while and VVSG 2005 as a committee you dealt with the concept of independent verification of voting systems and IDV as we called it back then, independent dual verification was proposed as a class of voting systems that produced records in such a manner that they can be verified independently of the voting system for their correctness.

Later in some other research papers IDV started getting called IV and we've used the terminology interchangeable. Currently I'll say the IV class is populated only by systems that use paper records that are voter verified which I'll discuss a little bit more in the next slide.

The committee here considered IDV for VVSG 2005 and opted not to mandate it. You included it and you included it more as guiding principles for building IV systems and with a signal that this would likely be required in future versions of the standards. That's where we are right now. We are at a point where we have to decide whether we are going to require this in the future.

Let me talk a little bit about voter verified paper record systems. Its common to think of voter verified paper audit trail systems right away when you think of voter verified paper records. The fact of the matter is there are other systems out there that produce voter verified paper records, op-scan being perhaps the best example. We've seen a report that basically estimates that almost fifty percent of the voters in 2006 used op-scan systems. A majority used paper based systems in general.

There are other systems out there, electronic ballot markers, electronic ballot printers which in a long of ways look like a DRE. They have the same sort of similar interface. They print out a nicer ballot. That ballot can then be scanned by an op-scan system.

As you can see the majority of states out there right

now require paper based systems. We have thirty-five states out there right now that use only paper. We have to write standards for paper based systems. That alone is a major undertaking.

We can't just say we have to write standards for them. We have to basically say that there are issues we have to address. A large reason it's a complicated issue is that poor implementations of paper place unreasonable burdens on poll workers and election officials.

One quick example of paper rules on VVPAT systems and they have their pros and cons. The fact is that they are difficult to handle. If an election official has to take a paper roll and in order to audit it, spread it out on a long table, that is complicated to do. Its difficult to do and its easy to make errors.

There are things that can be done that are pretty obvious in that regard. There are tools that can be included with systems to scroll through the rolls or otherwise make them easier to handle. Those are improvements that we know we can make and we should focus on them.

So STS recommends that NIST continue to development requirements to make paper based systems more usable as well

as accessible. In Nelson Hastings forthcoming presentation on voter verified paper records will address some of the issues and recommendations in this area from STS.

The HFP work that we are going to be considering tomorrow is also going to result in other improvements to paper based systems.

Before I conclude with the STS recommendations I want to address some of the work that NIST did in another part of independent verification. We've called that by various names, software IV, all electronic IV, but it is something that we wanted to work towards and that would be paperless approaches that are still independent verifiable. NIST worked on this issue and developed several very specific approaches and the aim was to come up with these approaches and derive from them some very general requirements that we could then put in the standards.

We thought we could do this. We worked hard on this issue and we decided as a committee that by doing this it would place unnecessary restraints on vendors' ability to innovate in this area and we just weren't ready.

Ultimately we concluded that more research in this area is needed and John Kelsey will address that a little bit

more in his presentation after Professor Rivest is through. Regardless STS believes it is important to push ahead and continue research in this area and these systems could promise a lot more usability, accessibility and security.

So, I get to the last slide which is basically an overview of the STS conclusions in this area. I'll summarize these and turn the podium over to Professor Rivest. The first recommendation as I have discussed is require voter systems that are independently verifiable and paper based systems that are in widespread use right now have this capability.

The second recommendation is don't stop there in any way. We have to focus on making improvements to paper based systems. There are many improvements that can be made, many obvious improvements especially with regard to the overall accessibility of the systems to voters and the usability of the audit capabilities for election officials. This is vital. We can't expect election officials to audit these systems if they aren't given the proper tools and if the systems are not reliable. There are many improvements that can be made. When we say voting systems that are independently auditable, we should assume that auditable

includes the property of being highly usable.

I have a final conclusion and that's basically the development of new approaches is needed. It's a good idea. We should continue to push ahead in this area.

At this point I am going to turn things over to Professor Rivest who will talk a little bit more about that.

DR. JEFFREY: Actually before that this may be a good time for the break. First are there any questions for John before we take a quick break? Okay. Thank you John.

Lets aim to be back about 10:15. I think that gives us a little bit more time for discussion as well on this subject.

DR. JEFFREY: Again, if I could have everyone's attention and ask everyone to please take their seats. We are going to be getting started.

Okay, welcome back from the break. At this point I am going to ask Professor Rivest to talk about software independence and encouraging innovation.

PROFESSOR RIVEST: Good morning everyone. It is a pleasure to see all of you again. It's a pleasure to be here. I was worried last Friday that I wouldn't be able

to speak because my voice was totally gone but I think I'm back and with a mike I should be able to make it now.

Welcome to the new members. Chairman Jeffrey also and Commissioner Davidson.

I guess I am back here because this was viewed as potentially one of the more contentious issues. I actually think in may not be and I will lead you through the discussion and see where we are.

This is two areas which I think deserve a bit of discussion of the TGDC, software independence and encouraging innovations. Commissioner Davidson already spoke to the encouraging innovation issue a bit this morning. I appreciate those preliminary remarks by her.

First I want to thank the members of the STS subcommittee and also the NIST team. I really found that there has been a lot of work, a lot of excellent work done, particularly by the NIST team, John Wack, John Kelsey, Rene Peralta, Bill Byrd and everyone else. Its been a marvelous effort. There was a lot of difficult issues to deal struggle with and the committee and NIST staff have worked really well, I think, to prepare these recommendations for you.

There is a number of different issues that the STS

subcommittee has prepared recommendations on. Two of them that I think deserve highlighting and special emphasis and discussion. One is software independence. I want to describe that to you and say what it means and we will have a resolution talking about that and recommending that all voting systems be software independent in the future. We will discuss that.

The next one is encouraging innovations basically saying that we don't know enough about how to build voting systems. We really need to encourage more innovation. There is a lot more we can do in terms of accessible, usability and security. We have two resolutions on that front. So that's the game plan. I've got about thirty slides and maybe take about thirty minutes or so to go through them.

A summary of the recommendations are these two. One on software independence and one on innovation. The first STS recommendation was recommending that software independence as requirement in the VVSG 2007. So we recommend that all new systems that are qualified under VVSG 2007 be software independent. I'll describe what that means and a little bit about the process.

A recommendation is that NIST in terms of development requirements focused primarily on the voter verified paper

record part of that because we understand that better. We also want to see if we can go paperless. Try to come up with new schemes that are software independent as well.

The second recommendation is about, which is encouraging innovation. We want to recommend that VVSG 2007 include a process for considering new software independent approaches such as end-to-end and recommends new innovative, possibly paperless SI approaches to be encouraged.

As Commissioner Davidson said in changing technology we want to try to see if the process that we have encourages innovation, encourages improvements and we have some particular ideas on how that might be accomplished.

Let's take the first issue software independence. This is a phrase which is, we haven't used it at the previous meetings. Its been a while. The phrase that corresponds most closely in our previous discussions was IV or independent verification. I'll make it clear what the difference is. I think this is a crisper term, a clearer term as to what we are talking about. It is actually very close to the idea that we have talked about before and which was discussed at some length in Appendix C of the VVSG 2005.

Software is a key part of most voting systems today.

It's a wonderful technology. I love working with software. I teach computer science. I teach students how to work with software. If gives you rich, flexible capabilities. Lots of ways of designing interesting, complex software to do interesting things.

However, it is really, really hard to get software right. That's one of the lessons of the last few decades. Really all software is buggy. When students write software its buggy. When I write software its buggy. When most companies write software its buggy. Bugs are a fact of life in software. If you look at the statistics, four or five bugs per thousand lines of code is sort of a norm. Some companies may get two or three, some get ten or twenty. There's a lot of bugs in software. If you have a 50,000 line or 100,000 line voting system, you are going to have quite a few bugs. You do the math. There is quite a few bugs still in the software and that's after extensive testing and careful development by a manufacturer or a team. Its really hard to get the bugs out of software.

From a practical point of view then, it really is impossible to write bug free code for a large system. Its just not something that – for a small systems maybe you can

attempt it but for a large system bugs are a fact of life.

So what about that? How does that relate to voting? When you think about voting systems in terms of how these bugs might affect the election outcome. You have these terms software independence (undecipherable) that reflect that relationship. A voting system we'll call software dependent or SD as we use the acronym. If an undetected bug, a bug that wasn't detected during the development process or in testing or a modification to the code, which corresponds, or a bug introduced maybe maliciously, the undetected bug in a modification to your software can cause an undetectable change in the election outcome.

That's sort of the worst possible result from a voting point of view. You have an election result that's wrong and you have no evidence to show you that it was wrong. There is no audit or post election test you could do that tells you if you have the wrong result. That's a software dependent voting system. It one where a bug can give you the wrong results an election can be stolen out from under your nose and nobody knows and nobody can tell.

Those are software dependent systems. It could be malicious. It could be accidental with a bug in the software.

It is dependent in a critical way in the software. The software is the stuff that, as I said, is really hard to get right. So its depending on this very marvelous, slippery stuff called software in a way that the election results depend on it.

A voting system is software independent if its not software dependent. If its not the case that software bugs can cause undetectable changes in election outcome. That's the notions that we are talking about. If you have a question about that now I can take one but I can go on and elaborate a bit further.

Software dependence, I think, is perhaps a more useful term that what we had in VVSG 2005 where we talked about IV. They are very close in meaning. We'll have some charts that talk about how they relate.

I think the term emphasizes the key issue that we see in STS tele-conference if you go back and listen to our discussions is the difficulty of trying to assure that software really is doing what its supposed to. So the software is the problem from a security viewpoint. Getting that software right, knowing that its right, assuring that its right, getting (undecipherable) the right software in

the system. We've talked about that before.

Managing the correctness of the software is the issue. Software independence is then a means for having election results in which we have more confidence because you don't rely on software in such an intensive way.

SI voting systems are those for which the correctness of an election outcome is not critically dependent on the correctness of its software. In practical terms SI systems have the property to test records and test results can be audited. So, as John Wack emphasized earlier, auditability is the key issue here.

A nice way that Josh Finley put it is, what we would like to see for elections is the ability to verify the election, not the system. I think there's a fundamental philosophical difference between those two approaches to security.

One is you try to build the system that you think is secure and then you trust the election results because you think the system is secure. So, you try to look at the software and say, yeah, this software looks okay therefore I should trust the election results. That's approach "A".

Approach "B" is you have ability to verify not just

the system and trust the election results because you think the system is okay, but to verify the election results themselves. You have specific evidence that that election, those election results are the right results. You are verifying the election specifically independent of whether the system has problems with it or not. That's an improve philosophy for looking at voting systems.

With a software dependent system, you have to assume that the system is correct. You have somehow been able to test it enough and it hasn't been modified maliciously or somehow along the way in order to trust the collection of the election results. That's sort of a fragile chain of reasoning because you have to assume somehow that you got adequate testing ability, adequate certification process, qualification process to know that the software is doing the right thing and that none of it has been changed.

As a side note software really means here and all the complex type technology that goes into a voting system, the hardware and the firmware and all the stuff because in some of the software it gets buried into the logic of hardware as well.

So, why not software dependence? Why can't we envision

going ahead with software dependent voting systems? The classing example of a software dependent voting system is the paperless DRE. What's the problem there?

The problem is the software is going to grow more complex in part because of the results of this committee. The work we are doing is putting more requirements on these voting systems. As a result the software is going to get larger and more complicated, more difficult to verify.

Arguing that the software is complex is really a research problem at best. It really seems to be impossible to verify in a satisfactory way that a large software program will always report election results correctly. There are places where people attempt this, the avionics industry and so on. People have very, very expensive means of trying to assure software is correct.

This is not an approach that sits well with the industry that we have in the voting industry. Given the cost structure that we have in this industry I don't think that kind of high assurance is viable.

I think, as you will see, if somebody wants to try that maybe we should arrange for them to do that within the innovation class but for the kind of work that we are seeing

in this industry, the kind of software development technologies and so on trying to get the software absolutely right, is beyond the state of the art. There is no vendor out there who is going to give you your money back if you discover a bug in the software. Its not going to happen.

So, there are ideas for building stripped down voting systems, getting rid of the operating system. The operating system is a large part of some of the problems. It has a lot of code. When you talk about four or five bugs per thousand lines of code you have an operating system with a million lines of code. There's a lot of things happening where you may not be happy with if you knew what they were.

Software dependence is just something which, frankly, we don't know how to write requirements for. That is the problem. Well, you try to say well here's a class of voting systems which the election results depend critically on the software. If that's the case, can we write requirements that would allow us to provide assurance to the American public that this software is going to be giving the right results all the time. The answer is no. We don't know how to test software to provide that kind of assurance. If think that's the message from NIST. There is no way that we can

write requirements that will assure the American public and the voters and the Secretaries of State that this software which is so critically important for the correctness of the election results are always going to produce the correct election results.

So the recommendation from the STS committee for this committee to model resolutions for this is that we go forward with a proposal that software dependent systems be excluded from our requirements. We don't write requirements that would enable the qualification of software dependent system. Only software independent systems qualify under these new requirements.

So, the big change then is that some systems currently in use, paperless DRE's in particular, which are software dependent, would no longer be permitted for new systems. This is a significant change. This may not be a surprise given what we have talked about before. We talked about IV systems and so on in the 2005, we talked about IV systems. I think we have a clear signaling that that was the direction we wanted to go in. This is the realization of that first step. There's a change we are going to have to discuss the ramifications of that. I'll discuss them in the slides.

So, voter verified paper record systems are software dependent. You have the audit trail that can provide a way of detecting when the software is misbehaving. Those would be allowed.

We would be proposing, primarily writing requirements for voter verified paper record systems. Paper isn't magic. There may be other ways of achieving software independence. There is a lot of ways on the horizon, in the research labs, in academia, people have (undecipherable) to achieving SI and those need to be encouraged as well. We see one good path to verified voter records. There may be lots of other things. I think we really need to see that those are explored vigorously. End-to-end systems are one of those and we talked about those.

Other approaches to SI, end-to-end systems, these are systems where you actually get stronger security guarantees than with simple voter verified paper records systems. With a voter verified paper record system the voter has some confidence that the vote made it as far as the ballot box but may not be so sure what happens after that.

With the end-to-end system the voter actually gets some capability of checking that his vote affected in the proper

way the final tally. There is some interesting techniques of accomplishing that without having the voter to be able to review how he voted. They use paper receipts, not paper records and they use cryptography and so on.

These are the early stage of the (undecipherable) now but they actually look very promising in terms of where you might want to be in a few years. Because they are new systems they may support voter usability and accessibility as well.

John Wack mentioned earlier software IV. This is another category of systems which are paperless. There are no paper records for election officials to maintain. Its like end-to-end. They are more software dependent systems. You have two systems which check on each other. So they probably fall in the software dependent class and so they make me a bit nervous for that regard but they hold promise because you can imagine maybe having two systems independently produce. There is a lot of debate within the STS and NIST about how those should go. They seem interesting.

So the recommendation is that we remain focused on paper because those are the ones we understand best. What does this mean? We have a proposal on the table that software

dependent systems be(undecipherable). This is the proposal we are making to all of you as the TGDC that we go over this idea that sticking with software independence is the right thing to do.

What does that mean about existing equipment? Does that need to be decertified? My understanding of that situation is that, no, it doesn't need to be decertified. The standards we are writing are for new equipment. It just means that new equipment would need to be certified under these guidelines that we will be writing. As the 2005 VVSG, current systems can be grand fathered.

I think its important to say also to states that have DRE systems now that requiring software independence doesn't mean that the STS or this committee is saying that the existing DRE systems are insecure. They may be insecure but they may also be secure. All they are saying is we can't tell if they are secure or not. You have a pile of software and trying to assess where we would actually provide the security that we want is the hard problem. Its not a condemnation of the systems in terms of security, its just saying that the assessment question for those systems is the hard part. We don't know how to write requirements which

allows us to tell that they are secure. If you can't tell that they are secure then we shouldn't be trying to get through the certification process.

Again, does requiring software independence of the VVSG 2007 mean existing DRE's need to be replaced immediately? No, and I give two reasons for that. First of all cost. Some states have invested their HAVA money in DRE's and it would be expensive to replace them if there is no reason to think that they are causing problems. Security may be fine to leave them a lifetime of use.

On the other hand there may be reasons for some of the systems to be replaced if somebody discovers a problem with them and the voters in those states wish to see something different. There is a class issue definitely.

Let me hurriedly throw out something. In security, repeating the point earlier, we are not claiming that these DRE's that are out there are insecure, just that it is very difficult to tell of they are secure or not. There is no reason to believe that the reporting of election results. The difficulty of telling whether its secure or not is the question you have to ask when you talk about writing requirements.

Can we as a committee write requirements that a testing lab could exercise that would allow them to tell whether a software dependent voting system was secure? The argument is that we can't. Its beyond the state of the art.

The STS doesn't know how to do it. NIST says they don't know how to do it. I don't know how to do it. I think its beyond this committee to say how to write requirement how to tell whether a software dependent voting system is secure. That's the reason for the recommendation.

If we don't require software independence, were are we? Its not clear. We don't know how to test for these bug free code. We would be back to testing the vendor to writing correct code perhaps. If that's where we want to be, the vendor supplies a software dependent voting system and we can't tell whether its secure really, we are trusting the vendor to write correct code.

Maybe if we could go to some avionics model we would have huge costs for development of a code. Its just a very different model for software development.

I think you could look at Congress and end the speculation because there is a motion in Congress to mandate voter verified paper trails. I think that's probably the

wrong thing to see happen. I think we can do a better job here. I think the software dependence is actually the right notion that paper trails are a means to software dependence and that by stepping ahead with software independence as the criteria we can preempt some of these motions in Congress would just say stick to paper trails. Paper trails aren't the only answer. There are other ways of achieving software independence I'm convinced.

Here's a historical chart of some of the notions. Particularly for the new members it might be helpful to see this. I've tried to show the relationship between these notions and how we got here.

Voter verified paper records include hand marked paper ballots, precinct con-op scans, electron ballot markers, ballot printers and DRE, VVPAT. Those are ones which are software independent. Voter verified paper records we understand them pretty well. They need improvement. As Commissioner Davidson noted earlier there are problems with VVPAT at times. Some of these other categories maybe have fewer problems but they all could be improved. That's part of what we are doing here, is writing better standards that relate to the voter verified paper records. Not whether

voter verified paper records, the DRE's, the software, you know, paperless DRE's (undecipherable) are out, of course.

There are other new categories that we are starting to see and this middle category things that are maybe not well representative of the market but which represent other approaches that look very promising. The end-to-end systems where the voter can see that his or her vote made it all the way to the final tally.

The software IV system. We have two systems checking each other. These are intriguing. So, the class that we talked about in VVSG 2005 of IV or IDV is really that class of VVR plus the other new class that's there.

Now this signal in the VVSG 2005 is basically the direction we want to be exploring in. Then as we got into it, it because clear that maybe this wasn't quite the right definition and that the issue of software dependence was really the problem. You know, trying to write requirements that would take a software dependent system and provide assurance to the public, the Secretaries of State and everyone else, that these systems really deliver accurate election results all the time.

We have the problem of software correctness and not only DRE's seem to have this problem but some of the software IV systems as well because they are basically software systems. There is no audit trail that's separate from the software.

If we move those out, the software dependent ones out, this is basically how the thinking evolved with our subcommittee. You have the IV class slightly strong but from a practical focus, not really that different because there really is very little market presence at the moment for software IV systems. So, the IV class is basically (undecipherable) and that really now, what we are calling the software independent class. So, the voter verified paper records and some of the other new categories such as the end-to-end which don't depend on software in this critical way is the class that we are talking about. This is what we want to focus on for VVSG 2007. The proposal would be that we ban or don't write requirements for software dependent systems. That's how we got to this stage and that's the basic picture.

I would like to move on. I could either take discussion here on this point or go on to the second part and they we

can have discussion at the end. I don't know how people feel.

MALE SPEAKER 4: Any questions for the first part of the briefing?

MR. BERGER: Something I haven't heard answered in many of the discussion, what is a threat model that you are working to?

MALE SPEAKER 4: If I could also ask that you identify yourself to keep the auditors happy.

MR. BERGER: Steve Berger.

PROFESSOR RIVEST: Good question. So the threat model is the starting point when you are looking at security. What are the threats to the system? Who are the potential adversaries? What kinds of resources do they have? What kinds of attacks might they mount?

When we are talking about software dependent systems, we are talking about threats to the software. They may be threats which are in some sense inadvertent. You have software dependence so you have a threat of just bad coding in the beginning and they are bugging in the software. So, that's one.

You have the threat of insiders in the process somewhere

having bad coding. Either at the vendor or somewhere along the distribution chain, changing the software. When you have dependence on the software, the threat model is any threat to the integrity of that software in terms of either its design or its delivery.

The Brennan (sic) Center report I think is probably the best place where that gets articulated in full detail where they talk about a variety of scenarios where either insiders or outsiders with access can attack the software. You have to start from just the fact the software is buggy to begin with. Being sort of a threat model is kind of unusual where you've got problems with the software that weren't even part of an attack in some sense. They just happen to be there and they don't produce the right results.

MR. BERGER: Any I accurately hearing what you are saying is you're maximizing subsystem security as opposed to total system security?

PROFESSOR RIVEST: I think the goal is to maximize the verifiability of particular election results. Its really the whole system, not even the system. To go back to (undecipherable) comment. Its not the question of evaluating the security of the system so much as verifying election

results. You would like to have confidence in each and every election result. If you are trying to view the accuracy of the election as a consequence of the fact that you have evaluated the system, that's Path "A". Path "B" is knowing that this election result you have confidence in because you got an audit trail for that election result.

MR. BERGER: I suppose then my question would be, of necessity if we become more software independent, we are becoming increasingly dependent on other components of the system. What are those dependencies and what's happened to the total security of the system? Have we perhaps become less secure because we are now more dependent on an even less reliable component in the system, for example, human error?

PROFESSOR RIVEST: So when you add a check, I mean typically things you didn't detect before. So you could take a DRE plus VVPAT and you just throw away the VVPAT or something like that, you've now got a system which checks less and therefore is more vulnerable.

When you are removing checks you've got the – I think that answers your question that you are talking about. The fact that an audit trail requires working (undecipherable)

usability issues and so on that have to dealt with. You are talking about security here and taking away checks never helps.

MALE SPEAKER 4: Any other questions?

MR. PEARCE: Philip Pearce, Access Board. I have a question. The resolution that you've recommended here that has been recommended here, have you considered the impact that that will have on state and local election officials? If you are recommending something that's different from what they are using now, using the DRE's without a paper trail, have you considered the impact that that will have on them because for sources they have to continue to use those same systems. I can you discuss that a little bit?

PROFESSOR RIVEST: Elections officials using the software dependent systems?

MR. PEARCE: Yes.

PROFESSOR RIVEST: We talked a little bit about that and I think the question is what kind of transition plan would they have and I think the slides answered that question probably as well as I can. I think Ms. Davidson and others may be able to speak to the issue of the transition issues.

As you change requirements over time, states need to adapt and we phased out punch cards, transition planning and costs would have to be incurred, most need to be scheduled appropriate and so on to but there certainly no dramatic instant changeover that needs to happen because of this. I think with all due deliberation and normal budgets cycles and so on these things can be accommodated.

MALE SPEAKER 5: Can I elaborate on that a little bit. I think that's an important question. The way I see the impact of these requirements would be if these recommendations were adopted they would affect new systems. So, they would not affect the use of existing systems, the jurisdictions would be able to continue to use existing systems.

The place where this has an impact is where they want to buy new systems in the future that were certified, submitted for certification after 2010. At that point then this would place a restriction that if they wanted to buy new systems that were submitted for certification after 2010, then those new systems would need to be software independent.

Again, I don't foresee a kind of major impact. We are

not talking about decertifying existing systems.

MR. SCHUTZER: Dan Schutzer here. I think I somewhat disagree about that. If I put myself in the shoes of somebody that had let's say invested in a DRE machine without verified voter paper trail, I now see I have two years to act to do something because I am, and I agree with the conclusion, somewhat vulnerable. I think it would probably be incumbent upon me to take a look if there was some kind of field up gradable fix to that machine which would mean today, unless some other process or approach is developed in time, some way of retro fitting it with a printer, for example. I think I might well consider doing that. I don't think there is anything wrong with that. I think that would be advantageous to consider that.

I would say that one thing we haven't talked about for the last couple of years here is the independency of the voting machines to all the systems that people processes and the voting process. I do think that people ought to start to think more about that and the interaction.

Number one you find that it's a cause of a lot of the issues that we are seeing in current elections thus the resolutions that we are putting in CRT. We might also find

some ways out of this dilemma also, some other alternatives for how you can get independent testing. I would say I do think it would be an impact if I was an election official.

PROFESSOR RIVEST: There may be some impact, you're saying in sense of the guidance this provides as opposed to the requirements and the kinds of style that election officials may feel motivated to adopt.

DR. JEFFREY: May I just also say that one of the curves that the TGDC is to provide the technical guidelines, the implementation and the time scale for that implementation is under the Election Assistance Commission and the decisions as to how the guidelines we produce may be rolled out in the future is a decision that is within the purview of the EAC with the guidance and input through their public hearings. Is that what you – I look to Commissioner Davidson if you want to add to that. I don't think that as part of the development of the guidelines that the TGDC would be providing specific roll out strategy.

MR. WILLIAMS: That was Dr. Jeffrey. He didn't identify himself. I'm Brett Williams, the NASAD representative.

We are talking in absolutes here. You say all software

is buggy. You say its difficult and expensive to test. The complex software for all practical purposes is impossible to test.

We don't live in an absolute world. We live in a probablelistic (sic) world. The question is can you test it to an acceptable level of security. An illustration of the fact that the answer to that is yes, is the banking industry. They move billions of dollars around every day with this buggy software without ever producing a single piece of paper.

MR. SCHUTZER: I would like to counter that. There's one big difference, its that with all this software we retain the identity of the individual and the parties to that transaction. We don't have this additional problem of the secret ballot so therefore I can go back, which we do and we have with the verified software issues crop up as they do in on-line banking and so forth. I go back and I verify, you know, I have that you did this. Did you indeed do this after the fact? You can come back and in effect of doing an equivalent of a verification but its easier for me to do because I know that Ron Rivest actually was the one that cast that transaction. I go back to him and I ask him that

questions. He will be very agitated if I find that he did something did indeed do. So, I do have to say that what I'm hearing, you know, based upon conventional wisdom of how well you can test this stuff is that its appropriate to do some kind of independent verification. Otherwise you can't really be sure. If you can't be sure, elections can be thrown into jeopardy.

MR. WILLIAMS: Brett Williams again. So maybe what we need to be doing is discussing the trade off between secret ballot versus voter verifiable ballots. If we could somehow dispense with secret ballots then it would be very easy to (people laughing).

MR. BERGER: Brett I believe you are starting us on a course that may be quite fruitful. A certain thought construct has been suggested about software independence. That may not be the best construct to work in. There are other – the discussion we've heard, I think is being made in the context of general computing and general computing software. There are other heritages of software, control systems, security systems, instrumentations that are much more deterministic, much more reliable and much more verifiable.

What I haven't heard discussed and perhaps we should explore it is, is it a stronger construct to talk about software independence or is it to talk about moving voting equipment, especially if the first recording of the ballot to a different software heritage where it is more verifiable.

MR. SCHUTZER: Dan Schutzer again. I think the software independence is a good way of thinking about it. What I was referring to is, and I'll give you something. I'm armchair engineering now, so I'm sure people will shoot holes in it but there are all different sorts of software people and processes in the election process. We've tried to get at that in CRT and we keep telling them we don't have time to do that. If we were to consider that, that there are these machines that tally the final vote and the transmittal of that vote as well as various machines in which you can authenticate and authorize individuals, I would attest that you think about that whole process.

I'll give you one example you can probably shoot holes in. You might get at the equivalent of a way of validating a vote. So supposing the voter is assigned an I.D. and a password, some unique way of identifying themselves as a voter. They go into a voting machine and they vote.

At that point they get a transaction code number that only they know. They can see that. They can write it down. They can do whatever they please. They go into another booth. That vote is immediately sent as a record with a transaction code number to the voter's identity and adds a record to another machine that's the machine that does the tallying.

That voter is then requested, again, we have to talk about practicalities. So when the voter logs on, he uses his transaction code number and he verifies that that record indeed is the record that's now going to be tallied and that record cannot be tallied until he indicates a check.

I'm just saying that there are ways, if you think about the fact that we do have multiple machines and software people and processes and so forth where that can be done.

There is all sorts of other checks you can do. You can certainly have election officials who can see that another record did go up without knowing what the content of that record is and there's another count in there. So, there's way if you start thinking about things we haven't been asked to think about yet.

In terms of how the officials run and the process the

machines is run that can maybe get around that. Of course, we are talking about something that would have to thoroughly vetted. We are a lot of experts but –

PROFESSOR RIVEST: I think we have the first two proposals here for the innovation class. These are new approaches which are not representative of what the industry is doing now but which I think we ought to try to support through the innovation class here. So, taking the software independence requirement doesn't mean that these ideas are excluded because I think you can also have those kinds of approaches explored.

They are new ideas. They are new approaches which need to be vetted.

Shall I move on to innovation? It was a good transition.

Clearly when you put this restriction on software independence people say well, maybe there's ways of doing it we haven't thought of yet. That's correct. There are other ways. We want to encourage this. I don't think we are any closer to figuring out what the right voting systems are than we are knowing what the right cell phone is.

Cell phones are in a state of evolution. You are going to see cell phones that are very different ten years from

now.

We are going to see voting systems that are very different ten years from now. So we want to encourage the voting industry to pursue innovative systems. We can hope for better usability, better security, better accessibility, all of the above. I don't think we are near where this system needs to be yet.

We might get, you know, paperless software IV systems to the point where we trust it, through the kind of heritage you are talking about, Steve to develop that way.

How do we encourage such innovations, feels this is important, feels this is an important complimentary piece to the software independent piece. This is trying to encourage innovation saying that, you know, voter verified paper records may not be the final answer.

There's lots of other ideas out there. Voter verified paper records. We can have requirements for those, but clearly within this group and the country at large there is a lot of cleverness and innovation that ought to be encouraged. We should plan for that. So, the goal here is to open the door within VVSG 2007 to new approaches and explicitly making that possible so that if someone comes

up with a better design, wants to get that approved under VVSG 2007, they don't just give up ahead of time because they say, you know, the requirements that its got to be SI.

It's got to be, you know, VVPR or something like that. You know, the door is open, whatever approach you come up with, they could make the case that this new approach really delivers the goods then we encourage them to apply and submit a design for evaluation.

The evaluation procedure would have to be somewhat special and that's a challenge that we face as a committee if we are going to design an innovation class like this.

So that's the proposal that we set up an innovation class like we have these other classes, but this innovation class is intended to encourage new approaches to be evaluated.

If we look at the chart we had before we sort of had, VVPR and if you look at the middle part of this page that's really the part where the action, is suspect, is going to be. Its going to be – these other new approaches, they are not well represented in the market yet. They may come from a different heritage. They may represent, you know, bring

several machines together which is what the software IV thing is that correspondence to what Dan was talking about.

I thinks there's this middle area where we would like to see activity happening. We would like to see new ideas coming forward, pilot studies being done. Companies being founded, whatever to promote this kind of work. This is where the future of voting may be. We've got some technology. We understand how to secure and how to write requirements for plus some other ones we know we can't write requirements for. These things in the middle. We have serious expectations that that's the place where things are really going to get better over time. I want to make sure that's enabled.

So, STS, TGDC could write high level guiding requirements for these classes. Obviously there is going to be a lot of different approaches so we need to have some fairly flexible process to evaluate these so a developer can submit a system to a testing lab along with some sort of very carefully documented argument that the system meets these requirements. Then the testing lab could convene a public hearing, expert review panel to review, to look at this approach and make recommendations followed by other

kinds of very vigorous testing. The hardest challenges we can put out there. Extensive open vulnerability testing and so on. These need to be thought through.

The idea of having an open door to new approaches together with a flexible, tough system of review I think might fit the bill and allow us to expect innovation encouraged and the systems that come through the process successfully would be probably different than the kinds of systems we have now but we would have high confidence in the security and usability, accessibility, etc.

That's the idea and obviously it's a start of an idea. As a committee we need to work together to figure out how to make this work well.

There's lots of aspects to this, you know, I note that – I just heard Peter Lyon talk recently at MIT. He's from the U.K. and there they have a Department of Constitutional Affairs and within that they have a section on electoral modernization which is actually running trials next May with innovative systems. They explicitly have a whole department working on innovation in election systems. They run trials. Maybe we should follow some of those. We do a lot of things in this Country too, trying out different precincts and

states trying out new things too. Its not unique to the U.K. but encouraging innovation by having pilot studies is part of that.

Paper is something that some people object to. I think that paper is by no means obviously required to come up with a secure system. It seems to be one of the better approaches that we know how to handle now. As we move forward these innovations we would like to encourage may actually give us nice paperless systems that provide all the security we want.

So, recommendations besides having the innovation class which was my recommendation number two, the first one was SI, the third recommendation is really a recommendation from this committee to Congress, I guess we could make such recommendations. Maybe somebody maybe can (undecipherable) if this is inappropriate but just the recommendation that Congress follow through with the grants for research on voting technology improvements that HAVA part 3. The EAC is to make grants to assist in carrying out research and development to improve the quality, reliability, accuracy, accessability for the security of voting equipment, elections systems and voting technology. If its appropriate

for this committee to make a recommendation to Congress say, you know, lets follow through with the funding of that, then I think that would be helpful in the spirit of this innovation support.

MALE SPEAKER 5: I actually think it would be inappropriate for us to make a recommendation to Congress. I think it would be fine to make an informal recommendation that there is innovation class research necessary but we report to the EAC and only to the EAC.

PROFESSOR RIVEST: Okay. So you do it informally or whatever but I think that that's something which would help.

Our resolutions, we can move into these and if you like we can vote on them here after further discussion. The first resolution was basically to require software independence in VVSG 2007.

The second is to include an innovation class. We wrote requirements for this innovation class.

The third resolution was the funding one which perhaps we should table.

I'm not sure what the best way to proceed is. I think having the wordings of these resolutions up and taking a

vote would be fine with me but if the committee wants to defer a vote until later or something we could also do that.

DR. JEFFREY: Let me open it up for discussion. Any questions or clarifications?

MS. QUESENBERY: Whitney Quesenbery from HFP. I just want to sort of put on the table that in Section 508 which is the Federal Accessibility Requirements there's a concept called Equivalent Facilitation which is somewhat similar to the innovation class. Those regulations acknowledge that when you write a regulations you are frozen – somewhere you have to finish it - and you are frozen at a point in time but that in the future new technology might be developed that would enable a vendor to meet a requirement but in a new way.

Although that regulations is somewhat flip because there is no certification, it allows vendors to submit what they also call a VVPAT but its voluntary – I can't remember but its an accessibility – it's a statement of the accessibility of their product. In it they can say well, we don't need this requirement in exactly the way its written but we need the spirit of it in a new way using new technology. So, there is already some experience within the regulatory

world

(**END OF AUDIOTAPE 2, SIDE A).**

PROFESSOR RIVEST: So that's, there's a precedence for this kind of thing you are saying and maybe even some support for doing or were you saying that it supplants what we are proposing to do?

MS. QUESENBERY: No, I think there's a president for it and certainly another agency is ably represent here. Perhaps the members of the Access Board can talk more in detail about it because I am looking at this from the outside but it seems to me that we have another example of Federal Regulation that leaves open a way to meet the high level requirements with need technology ideas.

MR. BERGER: If I may, Steve Berger. I think that's an excellent recommendation and I did have the chance to be on the advisory committee for Section 508. The equivalent facilitation though is predicated on the basis of the functional spec and in 508 there is a high level objective of the specification and then all the specific implementation requirements of those. The way the equivalent facilitation works is, if you can show that you meet the high level intent in some way that doesn't specifically meet all the detailed

specifications then you can be approved. So, I think if we were going to implement something similar to equivalent facilitation we would need to make sure we have that high level intent which had been as the criteria that you get judged against.

PROFESSOR RIVEST: I think that's right. For voting systems we have high level requirements clearly in terms of integrity of the count, of voter privacy, and so on and those would certainly have to be the starting point for that.

MR. BERGER: By the way, that also becomes a very helpful mechanism as a safety against any inadvertent flaws that may arise. So, if something meets all the detailed requirements, but clearly fails the intent is not secure, is not accurate, whatever, you can go up to the high level requirement and say well, its not secure even though it may pass the test. Its not going to pass.

MR. SCHUTZER: I think the concept for the independent source for verification as opposed to legislating a voter verified paper trail is moving in that spirit, its saying that the general idea is I would like to be somehow be able to verify the vote independent of the software and the DRE machine. So, if I can show I have innovated and I have some

equivalent way of doing that verification without the need for a paper trail, provided I can be vetted and convincing, then I can now use that. I think the resolution as it is being proposed sort of fits that bill.

MS. QUESENBERY: This is Whitney Quesenbery again. One other point, and I forget what meeting it was when we were discussing something and you said that complexity is the enemy of security. One of the things that occurs to me is that, I think you also said this, that a lot of the things that we need to do to make equipment accessible often adds complexity because it adds multiple input devices, it adds the ability to use additional technology with a core machine. Could you just talk a little bit about how software independence affects or plays into that discussion?

PROFESSOR RIVEST: I think those are things that I said and I think that as we add requirements software tends to get more complex. Steve Berger was talking about trying to do it from a different heritage to that input vote capture thing but we also have requirements on the vote capture side there. The goal here would be software independence all around so that any voter can audit their vote in a way that would allow them to be as independent as possible from the

software of the system.

MS. QUESENBERY: So does that in effect kind of separate the input mechanism from the counting mechanism somewhat? That is, if there is a verification step of some kind in the middle does that suggest that then the input mechanism could be more complex and not damage the security of the system?

PROFESSOR RIVEST: Yes, exactly right. If you have a verification step in the middle of the process, then I think you obviate the need to trust the software of the input process as much. So, you end up with software independence in a nice way.

Some of the systems already on the list are like that, the electronic ballot printer (undecipherable) have exactly that character.

MR. SCHUTZER: I can elaborate on an example from my world. We are sitting there and you look e-mail spoofing, for example, things like that, fishing. There has been complex solutions to try to solve that problem. May of you have seen it. Some of the solutions like where you suddenly see some graphics that show some images of letters and before I can send out the e-mail I want to make sure I’m a human

and not a robot, so I'm typing in these images that I'm seeing, i.e., let's say a machine couldn't do that.

It turns out that one of the ways that the fishes get around it I am told, is there is an ability for disabled, maybe people that can't see, to have sound, audible sounds for this sort of thing and so they run down to that because then they can decode the letters. They don't have to look at the graphics. They are listening and doing the voice recognition so to speak.

So this complexity that sends, you know, is the enemy of security but if you do something simple like you say independently of that I am going to verify anything that gets done, by going back to the individual like in banking and say did you indeed authorize this $10,000.00 transaction, in another channel, then you have gutted around those problems and you still can allow to have the disabled interface as well, the disability interface as well as the graphics interface.

PAUL MILLER: As Paul Craft's replacement I will always try to introduce myself before beginning.

I might be the, well, I've got questions about the SI and I apologize if this is the wrong time.

PROFESSOR RIVEST: Its exactly the right time.

PAUL MILLER: I will appeal to the fact that I'm a new member of the panel to justify it.

To move it away perhaps a little bit from the controversial area and what does SI mean when we are talking about a paper based system such as optical scan? In particular, the question that I am asking is, is a system software independent when it is used in the field, if the system is not audited, number 1, or number 2, the people using the system, probably primarily because of disabilities, aren't able to verify that what was put on the ballot in the first place was in fact what they intended? Is it a software independent system?

PROFESSOR RIVEST: Good questions. The first question was about auditing and whether a system was SI if its not audited. The definition is intended to give the yes answer for that.

The system is SI if it produces evidence that is capable of being examined afterwards and disclosing. It's a capability of being audited that we are talking about here. The system itself, the auditing procedures outside the scope of what this committee does. We don't specify audit

procedures.

So when a vendor submits a system to be evaluated, he is not submitted the audit procedures as well as part of the system that gets certified although we may require some documentation of that. The actual frequency in which they get applied and so on. Many are moving in that direction.

The short answer to your question is, you know, the system is SI if it produces the evidence of detecting errors that might be caused by bugs in software or even malicious software and so on.

A system can be misused and if you don't do the audits you are misusing your system. The system is geared to provide the auditing capability and that's important and if you are not doing the audits that are possible to be done with an SI system, you are abusing the system in terms that you are not taking advantage of the capabilities it offers.

The second question was about SI for voters that may not be capable of verifying their vote in the same way. The definition of SI as drafted and we can modify this under discussion as appropriate, is that the ability for normal voters to verify their votes and the intent is to make the system be SI for all voters, but the system is defined in

terms of the definition is to have a class is for voters without disabilities that would be the intent.

There are different systems for different voters in some sense.

PAUL MILLER: If I could follow up on that question for just a minute. There are systems out there that probably people, only people who have disabilities would use. The ballot marker devices come to mind. In that case even though they in fact produce paper that theoretically could be verified, unless you are able to visually see the paper and handle the paper you would not be able to verify it and a person who is able to see the paper and handle the paper would not use that system.

MR. BERGER: I personally feel we are trying develop interesting systems for all voters to use but to take your question –

PAUL MILLER: I'll expand on that for a minute. I obviously test and work with these systems and as clumsy, I shouldn't put it that way. It takes a great deal of time to complete the process of voting by ballot using the ballot marker system. A person who can do it, has the capability of doing it, can do it much faster than they would be using

that device.

PROFESSOR RIVEST: We are probably talking about a definitional question. The main proposal is that a system be SI for normal voters. If you have a system which is designed primarily for voters with disabilities, I think this committee then has the responsibility to try to figure out where the exact boundary of the envelope is and how you want to do it. I think that the goal should be as much as possible for all voters, that the system be software independent and for some voters you may need accommodation or other approaches to try to approximate that approach. I look forward to working with the HF committee to figure out exactly how best to draw those lines.

They are not easy questions, all of these and I think the goal here is to serve all voters in a way that provides the maximum amount of usability, accessibility and security. I think in the security system if you can achieve software independence for all voters, that's where you want to be. We may realize what's the best or approximated or accommodated.

PAUL MILLER: Thank you.

MR. WAGNER: I thought this was a really important

point. I wonder if I could elaborate a little bit on what Ron said, my take on that.

I think the intent was absolutely that electronic ballot markers, electronic ballot printers, these other devices would qualify, would meet the requirements. I have a slightly different way of thinking about what the SI requirement says.

I think of the SI requirement as a requirement that you be able to verify or to audit the overall election results as a whole. Its not talking about a specific right to any one particular voters. Its talking about being able to verify the election results as a whole. For instance, its likely if we are talking about voter verification as one approach to SI, its likely that some voters will verify their vote carefully, some won't, some may not verify it all. That's okay. These systems can still provide software independence even if not all voters are doing that.

PROFESSOR RIVEST: I think its important that all voters, to the extent we can deliver that, have verification capable and make it software independent for all voters.

MR. WAGNER: Just to add to that, yes. I think its to all our benefit to increase the accessibility of the

verification capability to the greatest extent that we can. I don't think that conflicts with SI at all.

MS. PURCELL: I think one thing we have to keep in mind as we have talked about a number of times on our calls is that what we are recommending to the EAC and hopefully will be adopted, is not for the present day, its not for today or even tomorrow's elections, but for the future. It seemed to me that we were all rush to judgment on after the 2000 election with the establishment of having something almost immediate to give to the election officials and the voters.

We added things to machines that we wouldn't normally do in a short time frame because we had to have them ready by the 2006 elections. I would hope that we are looking forward to making significant changes and, in that respect, changes that maybe we don't even know about yet but will be designed for future election systems.

DR. JEFFREY: Any other comments? Okay. There is a resolution that has been offered up. Could I ask either Allan, you've got the whole thing. Its up there.

I think there is a piece that I have in writing that is not up there. It's a second paragraph.

MR. EUSTIS: I can read it.

DR. JEFFREY: Okay, why don't you read it for the audience.

MR. EUSTIS: This is Resolution 02-06 offered by Dr. Rivest, titled Software Independence in the VVSG 2007.

"The TGDC has considered the types of voting system architectures to be included in the next iteration of the VVSG 2007 and has made the determination that it would be unwise to allow for voting systems of the software-dependent class, in which the correctness of the election results is dependent on the correctness of the software, to be certifiable under the next iteration VVSG 2007. The voting systems that can achieve certification under the next iteration VVSG 2007 should be of the software independent class, in which a previously undetected change or error in the software cannot cause an undetectable change or error in an election outcome.

"Therefore, the TGDC directs NIST, in its development of VVSG 2007, to draft requirements for voting systems of the Software Independent class, and not to draft requirements for voting systems of the Software Dependent class."

So that's the proposal.

DR. JEFFREY: So there is a Resolution. Do we second before we debate? Discuss and then second later? Okay. So is there a discussion on the specifics of the Resolution? Steve.

MR. BERGER: You know, I'm –

MR. WILLIAMS: Would this Resolution in effect disqualify all current voting systems except optical scan?

PROFESSOR RIVEST: No.

MR. WILLIAMS: Which ones would it not?

PROFESSOR RIVEST: Pen marked paper ballots, end-to-end systems, for example.

MR. WILLIAMS: They don't exist right now. My question was, of the voting systems that are currently in use, if this Resolution passes, which ones would satisfy this?

PROFESSOR RIVEST: We have, you know, voter verified paper records, of which the majority of the op-scan does and the op-scan either produces the number of ways either hand mark or, --

MR. WILLIAMS: I'm looking ahead but in reading the papers for this meeting, I believe in another place that your committee is recommending that the current VVPAT voting systems also might be approved.

PROFESSOR RIVEST: No.

MR. WILLIAMS: (undecipherable)

PROFESSOR RIVEST: No, the VVPATs are also in the class.

MR. WILLIAMS: All right but aren't you opposed to that paper reel?

PROFESSOR RIVEST: As an SI class they qualify as SI. That's the (undecipherable). So, whether we, as a committee, are happy with the paper reel is a secondary question. Obviously paper reels have their issues and that's not the question that's being addressed here.

The VA plus VVPAT, whether its paper reel or independent qualifies as SI and would be allowed under this instance. So, VA plus VVPAT, optical scan and marked paper ballots, electronic ballot printers, electronic ballot markers, all of these systems where the voter gets to see a paper record and verify that will qualify.

MR. WAGNER: I wanted to just to elaborate a little on what Ron said. Its an important question. I think you deserve an honest answer. On the VVPAT continuous roll, what the white paper with the recommendations of STS, we'll get to them later but you will hear, recommends allowing

continuous roll VVPAT. It is not recommending forbidding them.

MS. PURCELL: On thing I might ask that maybe we would change in the last paragraph, rather than the way its stated: “Therefore the TGDC recommends that the EAC direct NIST” and I believe that’s the proper format that we have to go through.

PROFESSOR RIVET: Actually I would be happy with the TGDC directs the STS, the Security and Transparency Subcommittee in the development of the VVSG. So if we substituted the STS, that would satisfy, I think. Instead of NIST substitute STS.

DR. JEFFREY: So, directs the STS.

PAUL MILLER: I started to say earlier I might be the only person present who has been in the roll for eleven years of managing and the deployment of voting systems. I did so in Keene County for eleven years. I am very aware of just how difficult the degree to which that election officials are required to test these systems to ensure that for a specific election that the system has been set up correctly, that its going to count the votes correctly and the pressure that places the logic and accuracy tests that

are conducted and so forth.

Fortunately with SI I don't see any of the need for that going away at all. I think, in fact what we are adding and have added in the State of Washington, because we did, by the way, in the State of Washington, we have added the requirement that they have a paper trail and that there be a 4% audit and I participated in that decision, so I agreed with it, but I agreed with it as being right for the State of Washington, not necessarily as the right solution for every state in the country.

The problems that we were concerned about as we were wrestling with the decisions are very real. With the paper audit trail we have added to the complexity for the poll workers to handle. We have reduced the reliability of the equipment in the field and from an election administration point and I think from the concerns, it should the concerns of our standards, those are also important issues that need to be brought into play.

I am concerned at this point that we are imposing a requirement when I'm not sure that we have really proven that the processes that state election officials have used for a few decades now of testing and verifying that the

systems work before they deploy them is failing. Now we are adding another requirement that they also be able to not only test before they deploy them but that they be able to audit them, and in fact audit the system after they deploy it. I'm asking you to respond to that.

PROFESSOR RIVEST: I can respond to that. Its clearly the case that adding an audit capability is adding additional mechanism, adding additional work. The question is why is that there? The reason that its there is that the software dependence of these systems is such that, from the certification, from the testing qualifications point of view you can't tell –

PAUL MILLER: I appreciate that argument at the National level but at the local level when they deploy the equipment they are testing for that specific election that that system is going to work right.

PROFESSOR RIVEST: I don't know the test procedures that you have in mind but, I think that testing, its well understood that testing only gets you part way there with software correctness. Testing is something which provides some assurance that things may work well but its not a panacea.

You can’t test every logic path through a piece of software. Doing logic and accuracy tests on a few handful of candidates doesn’t exercise all of the cases. Maybe you have voters coming in who want to do, you know, straight party voting with a large font and other things.

The combination of choices that the voter can make is rapidly exploding as we improve the user interfaces for usability and so on. I take issue with the assertion that the testing is really any kind of comprehensive check on the accuracy of the software. Provide some assurance, provide a good gut feeling but its not from a security viewpoint there may be explorable abilities that just aren’t caught by the testing that we need to be worried about. It’s a question of where you want to be. Do you want to have a system where it looks okay, as people who work with the software say. It looks okay at first glance but when you really dive into it, carefully the testing seems to work on the test examples and people that develop software know that that doesn’t cut the cake a lot of the time.

Testing is a tool but its not, it doesn’t provide the back up, the recovery capability when something goes wrong. When the audit trail is there, it provides a recovery.

When you have something that's gone wrong and voters say, votes are flipping or whatever, you've got a paper trail they can look at or some other means of verifying their vote. If the testing fails to catch a bug, the audit trial provides a recovery mechanism that allows you to recover that vote in many cases. Not always. The paper trail has often been damaged as Commissioner Davidson said and you have to make a judgment call there. It provides an additional capability for getting it right.

MALE SPEAKER 5: I would like to ask Commissioner Davidson if you have a comment or question?

COMMISSIONER DAVIDSON: My comment is not on the issue that we are talking about. My comment is, hopefully to clarify to the public and I know the committee already understands it, but when we say VVSG 2007, I think that the public thinks that we are changing what we already have in place.

The VVSG 2007 that is being implemented it has to be completed at that time. If we could talk about the new iteration or some place define what we are talking about in the future is the new iteration that you are presenting the VVSG of 2007.

If we can have a definition, someplace or in the resolutions speak about the iteration that somehow or another make it clear that we are not changing existing what we have, the VVSG of 2005 that's going to be completely implemented by 2007.

I think that is confusing and I'm afraid the press and the public is not really aware of all the different technology or aware of all the different time frames that we are dealing with and what we actually are trying to accomplish. I feel like if we could clarify that in some way it would be helpful.

PROFESSOR RIVEST: Is there a wording change in the Resolution that would affect that?

COMMISSIONER DAVIDSON: I don't know if it has to be in the Resolution, maybe someplace, a statement somehow or another that can be make in the committee that this is, you know, someplace on the web that what we are discussing.

I really think that its been perceived that these changes are going to be made by 2007 and this, we know, is not the case at all. It won't even be reviewed and adopted possibly until 2008. So we need to make sure that this is not a confusing issue to the public and the press and everybody else.

MS. QUESENBERY: Could we amend this by simply saying “therefore the TGDC directs STS to draft requirements for future voting systems.”

MALE SPEAKER 6: If you want to in a public meeting tell them this will be in effect by 200___.

MS. QUESENBERY: We don’t actually know when it will be in effect.

MALE SPEAKER 7: And the meeting does not have public comment in it at this point.

MR. WILLIAMS Maybe we need to quit calling this the 2007. Go with 2010 or 2012 because that’s –

MS. QUESENBERY: Or just for the next version. We as the TGDC know when we are going to deliver our recommendations. We have no idea when it will be either adopted or implemented.

MALE SPEAKER 8: May I make a friendly amendment then, the development of the next version of the VVSG, would that be better?

MALE SPEAKER 9: So I think the suggestion is every place where it says VVSG 2007, it would substituted next version.

COMMISSIONER DAVIDSON: Next version, next iteration,

whatever, you know. This is Donetta Davidson again. The next iteration we have called it in the past. Whatever we want to do there, just so, you know, its really not VVSG until after its adopted. So, I think we talk about the iteration that will be proposed, that type of thing.

MALE SPEAKER 9: So, the recommendation is that the next iteration every place where it says VVSG 2007.

MR. WILLIAMS: I be happy with those as a friendly amendment.

MALE SPEAKER 9: Okay.

MR. BERGER: I'm very uncomfortable with the specific focus of this resolution and I think many observations there is no fundamental superiority of one type of system over another, only where the vulnerabilities and possibility of problems reside. It seems to me that the concept of software independence puts the focus one place where to totally improve the security of the system we need to put all the systems under equal scrutiny.

I personally would like to suggest that what we are really after is voting systems that are auditable and develop a permanent record. Obviously paper systems are arguably not a permanent record in that they can be compromised in

a number of ways. You can swap ballot boxes, you can destroy the paper in any number of ways. So as we craft this resolution, I would strongly recommend we craft it in a way that puts equal pressure to have total system security equivalent as opposed to just move the problem out to where now what we have is more dependence on physical security of the system.

MR. WAGNER: I'd like to speak up in strong support of the current Resolution. I think the current Resolution recognizes the limits of the current state of the art in assessing the security of large software systems and I think this focus on software independence is exactly the right one and so I think this is very, very important. I think this is the single most important thing that we could do for the security and the transparency of the voting systems, the next generation of voting systems.

DR. JEFFREY: Any other comments or questions on the specific Resolution as amended in front of us? Okay, there's a resolution in front of us, is there a second?

The resolution has been seconded. Parliamentarian do you do the vote or do –

as modified. Is there a recommendation for unanimous consent?

Any objections.

FEMALE SPEAKER 4: Object.

DR. JEFFREY: Let’s do a roll call vote. I suggest the Parliamentarian.

PARLIAMENTARIAN: This is Resolution 02-06 as amended. Williams.

MR. WILLIAMS: No.

PARLIAMENTARIAN: Williams votes no. Berger.

MR. BERGER: No.

PARLIAMENTARIAN: Berger votes no. Wagner.

MR. WAGNER: Abstain.

PARLIAMENTARIAN: Wagner abstains. P. Miller.

PAUL MILLER: No.

PARLIAMENTARIAN: P. Miller votes no. Gale. Gale is not responding.

Mason.

MS. MASON: No.

PARLIAMENTARIAN: Mason votes no. Gannon.

MR. GANNON: Yes.

PARLIAMENTARIAN: Gannon votes yes. Pearce.

MR. PEARCE: Yes.

PARLIAMENTARIAN: Pearce votes yes. A. Miller.

A. MILLER: No.

PARLIAMENTARIAN: A. Miller votes no. Purcell.

MS. PURCELL: Yes.

PARLIAMENTARIAN: Purcell votes yes. Quesenbery.

MS. QUESENBERY: Yes.

PARLIAMENTARIAN: Quesenbery votes yes. Rivest.

PROFESSOR RIVEST: Yes.

PARLIAMENTARIAN: Rivest votes yes. Schutzer.

MR. SCHUTZER: Yes.

PARLIAMENTARIAN: Schutzer votes yes. Turner Buie

MS. TURNER BUIE: No.

PARLIAMENTARIAN: Turner Buie votes no. If I may confer with Dr. Jeffrey, please. At the present time we only had six voting yes. The motion fails.

DR. JEFFREY: Should we proceed to the next resolution?

PARLIAMENTARIAN: Yes.

MR. EUSTIS: The second resolution corresponds to the innovation class and let me read it. "To spur development of new and innovative secure voting systems the TDGC directs," and again we will replace this with STS, "to include in the next version of the VVSG a new class of voting

systems, referred to here as the ‘Innovation Class.’ The TGDC direct STS to investigate high-level, guiding requirements for systems in this class for the purpose of providing system implementers with a path towards achieving certification to the next iteration of the VVSG. STS should also investigate approaches for reviewing, testing, and certifying systems in this class. These approaches could include convening a review board to review submissions and performing expanded open-ended vulnerability testing on systems submitted for certification.”

DR. JEFFREY: There is a resolution. Is there any discussion? Any questions, comments? Seeing no questions or comments is there a second?

MR. WILLIAMS: I’ll second it.

DR. JEFFREY: Okay there is a resolution that has been seconded. A motion for unanimous consent. Any objections to the unanimous consent?

MR. WILLIAMS: I move for unanimous consent.

DR. JEFFREY: Okay, without objection then it passes by unanimous consent.

That’s the resolution on innovation classes amended substituting next version for VVSG 2007 and STS for NIST.

Thank you very much Professor Rivest. Next up I believe is John Kelsey.

Just to clarify the first vote by Parliamentarian Rules it takes eight positive votes to pass a resolution is case there is a question on that.

MALE SPEAKER 10: If I could clarify real quickly, we have fourteen present so eight is one more than half.

MR. KELSEY: Okay, Allan are you ready? So, I think you tell me this doesn't work so let's see. Oh, it does. Its magic.

I'm John Kelsey. I'm a NIST employee and I'm going to talk about electronic IDV. We talked a little bit about this. Ron talked a little bit about this. I wanted to go into a little more depth about what we've looked at and kind of where we are with things.

Well, it worked a second ago. Okay. There we go. I want to start with this picture. I have to apologize. The slides that you have don't have some of the pictures. I always tinker with my slides until the very last second and so I didn't really think about how it was going to affect the print outs. So, I apologize for that.

The picture is kind of interesting. I'm sorry? There

should be. That's bad because its losing the picture. We have a huge room full of engineers here. We can probably do this. That's losing lots of information.

MALE SPEAKER 11: Make it the larger size to fit the screen and so back to that.

MR. KELSEY: Okay. All right. So lets live with what we've got rather than trying to fix on the fly. Something we probably do a lot with voting systems.

So, this is sort of a very simplified picture of a voting system. You have voters that come in and vote with the voting machines in different precincts, different polling places. As voting machines collect the votes they eventually send records in to some central computer, tabulation center or something. That tabulation center does magic. That tabulation center adds those totals up and gives you the final totals of the election. The important thing to understand about this, most of this is actually fairly, its not so hard to audit. Its not so hard to check to see that the results are correct because of you have all these intermediate totals from the different voting machines, the different precincts and you have the final totals you can just do some addition and check that those check out.

Using, say digital signatures and some of the other stuff that we are doing in the current draft, you can make sure that the records that came out of voting machines are the records that got here and were included in the final total.

The part that's hard to audit is this interaction between the voter and the voting machine. As Ron said, the reason why its hard to audit is because it has to happen sort of in a bubble of privacy.

We can't ask the voter afterward, hey, did you vote for Smith or for Jones. That's really the thing we are trying to address. That the thing we want to address with IDV.

The question that we started with about two years ago was could we write standards for all electronic voting systems that we could audit or we could audit that part between the voter and the voting machine. By that I mean we would have an independent record beside just what the one computer or one system told us of what the voters had done.

The first part of the answer is we think its possible to design such a system but it's a research problem. Its not something where we can just say here it is and just use

existing off the shelf technology and have something we are confident in. Even if we can design one such system, we don't know enough to actually write the standards for all such systems. Trying to write those standards right now would wind up giving us, trying to lock in a very preliminary understanding of the problem and probably block a lot of innovation.

So, the high order bit of this talk is we probably don't know enough to write standards for the IV systems yet even though we think they are very promising. We would like to see them in the future.

How do you make a voting system auditable in this sense? Well, the obvious solution is paper. That's kind of what we have now. We know the problems. So, trying to do this without paper, you wind of with some sort of independent record.

Your goal is to make an independent record of the voter's interaction with the voting system beside just what the voting machine records. You use that independent record to, your audit it, you just use it to keep the voting machine honest.

Let me talk about three really broad approaches we had

to this, that we looked at and then talk about some of our conclusions on this. This was the first thing that we look at. This is dual process. In (undecipherable) Cal Tech report, the talk about a system like this. So you have the voter interacting with two different machines.

This is one of the places where the pictures matter. What you see here is the voter interacting first with the voting machine and then with a second system that does the verification. They voter has to interact with two different systems somehow. That's the whole idea of the dual process model.

The goal is when the voter interacts with this first system, he maybe, for example, makes some selections and then with the second system he verifies those selections. Each of those systems makes a record of that and then the audit checks those two against each other.

The idea here is, if either voting machine or the verifying machine were compromised, we would catch it as long as the other machine was honest because we would have different records. They wouldn't agree.

The threats you have to worry about here are, first of all are the machines and the records independent? That's

a big problem with these systems. In other words if the voting machine and the verifying machine were manufactured by the same company, the code was written by the same programer, you might not actually have any independence between these two.

The other thing is you have to ask whether the voter actually checks the verifying station. There are variations of this, but that's a broad problem you are going to have with this sort of system.

I believe in the materials we sent out, we had a couple of systems that we had talked about and kind of proposed and done some analysis. One of them was this (undecipherable) with a view screen. The idea here is if you imagine, something very much like (undecipherable) with VVPAT but instead of the printer, if you imagine just, instead of bolting a printer on this side, you bolt a second machine, a second computer on this side with a screen. Then you could imagine the voter voting on the regular voting machine and then verifying on this sort of view screen. To audit it, you just compare the records.

If you are going to look at a system like this, you have to this about how you would attack it. The obvious

way to attack this sort of system is by compromising both. If you can compromise both of those systems, then the audit becomes meaningless. The same way that if you could both compromise the voting machine (undecipherable) with VVPAT system and also intercept the paper trail and replace it. That wouldn't be a useful audit anymore.

The kind of more interesting attacks here come about because if the voter isn't paying attention to one of those systems, he's interacting with two different systems. If he is not paying attention to say the verification station, then the voting station might just mis-record his vote and he might never notice. That's also very similar to something that happens, one of the attacks you worry about with VVPAT.

So, second approach to IVV that we have thought about was the idea of adding a witness device. The idea is the voter and the voting machine are interacting and the witness device is sort of tapping the line and recording the interaction. The goal here is then, all of this interaction between the voter and the voting machine happens normally, there is no change in the process of voting. We just record it. The witness device produces a record, the voting machine produces a record and you can cross-check those to make sure

that the records votes correspond to what was actually displayed to the voter.

There are sort of two interesting questions with this sort of system. Number one, the same as before, are the witness device and voting machine really independent? Are they really meaningful cross checking each other if they were made by the same company and the program was written by the same person? You have that one dishonest person who could compromise both systems.

The other question is whether the witness device is actually getting a good read of what the voter is seeing. If you could somehow as an attacker confuse the witness device and what the voter is seeing, then you have an attack on the system.

An example of this is, this has been proposed a couple of places. You can take a normal DRE with a standard VGA interface for the screen, you could tap that VGA interface. It is sort of like the t.v. signal, high resolution. You could tap that and you kind of splice that wire from the computer to the screen and feed that into a box that was recording it.

So you have this witness device that’s tapping into

the screen, its seeing the same thing that's being displayed on the screen and also you could have like some sort of keyboard or buttons and that would also be spliced into the witness device. If you did this, you would be able to record the interaction between the voter and the voting system without ever affecting the voter's experience. You don't make the voter do anything else.

You just have them interact with the voting system and that all gets recorded twice independently.

To audit that you could, for example, randomly select a few hundred voting sessions that were recorded and have a human watch the session and make sure that it actually recorded the right vote.

How you attack this sort of system. First of all there is a whole set of attacks who worry about, that involve getting the voter to see something different or perceive something different that the witness device. For example, if you could flicker the screen in some way so that the VGA display showed something somewhat different. The voter saw or perceived something different than what the witness device recorded. That would be an interesting kind of attack.

Also, of course, if the witness device and the DRE were

kind of conspiring, if they were both compromised at the same time then that wouldn't be a useful audit.

The last thing, and this is sort of an idea that is implicit in a couple of people's designs is to try to come up with a physical record of the vote that's not paper. We know how to make a paper physical record and we have a lot of voting systems based on this, might be whether there's another way to do a physical record of the voter's vote.

So, in this case you would have some physical process that either the voter was interacting with the voting machine and the physical process was recording it or the voter might be doing some physical process like using a lever machine and then a computer might be recording those lever pulls and button pushes or something. You would have a physical record that was not susceptible to software tampering and also have the electronic records.

A kind of neat example of this, I don't know how usable it would be generally, but Ted Sulker (sic) an MIT professor had proposed a DRE with an audio belt, where the audio belt was always part of the interaction between the voter and the voting system. The suggestion was that you could use sort of a witness device, you would record the audio channel

on magnetic tape, on analog tape.

The nice thing about recording it on a fairly simple analog device is you could physically inspect that recording device so you wouldn't have to worry so much about subtle software attacks changing what was recorded. You would still have to make sure that the recording was right and you still have to worry some about tampering, but hopefully you would be able to use your inspection task. That's sort of the idea there. That's kind of interesting.

Basically if you think about attacking that what you would do is you would try to maybe replace, you would put something in the line between what the voter was hearing and what the tape recorder was getting. You could tamper with the magnetic tapes the same way you could tamper with paper. Also maybe you could mislead the voter by giving video feedback that was confusing when you also heard the audio feedback or something.

Those are three approaches that we have looked at some depth. There actually are quite a few other people, other things people are thinking about, doing graphic protocols, doing --. Dr. Wagner has done some interesting stuff with trying to minimize the amount of code that you are trusting.

Some of the stuff that you were talking about earlier, Steve Berger was talking about, I guess boiling down the trust to a very small set of code and then testing that.

There are a lot of other ideas that don't look much like this. What we are talking about here is really making sure we can audit this interaction from the voter and the voting machine. A lot of those don't quite fit into our category here although they might still be interesting.

So, the kind of question you might ask is, why can't we write standards for it? Of course, the answer is because this is a research problem and its really hard to write standards for stuff that you are still doing research on.

Basically there are a few people that have built prototype but mostly it is just researching. You can get a good paper out of this and submit it to an academic conference. That kind of implies to you that this is not quite ready to write standards for.

One of the big problems we run into with these systems, especially the ones that seem the easiest to build and use, is that you tend to have multiple software systems that are

auditing one another. You haven't gotten away from the problem of verifying software. You have just said well, I have to verify that at least one of these two pieces of software is not cheating.

That's not a whole lot easier than verifying one piece. You don't really fundamentally change the kind of problem you are facing. The independence of these devices is really problematic because they are probably stored in a warehouse together. They might be bought from the same company.

So, kind of the biggest issue to my mind about trying to standardize these is just that we don't know what the progress will be in the next five years on this. If we tried to write standards for it we would probably freeze the progress out. We wouldn't know enough to write standards that would include the good stuff.

At a high level we think these auditable, electronic voting systems are worth investigating but we don't think we know enough to write standards yet. That's kind of the high order bit of the talk.

Do we have any discussion or questions?

MALE SPEAKER 12: Any questions or comments?

MALE SPEAKER 13: Yes. One question. You talked

about doing research. Have you been able to contact or find examples of any election systems anywhere in the world that are auditable but do not use paper systems?

MR. KELSEY: I believe there is a Spanish company called, SkyTel (sic) that does something like this, at least somewhat like the dual process model that we were talking about. I've seen just product documentation on the web. I haven't seen devices or checked them out.

I think that might be the only case I could think of. This isn't something that I know of anybody who has done at great depth. Like I said, I think this is mostly research at this point.

MALE SPEAKER 13: It was my understanding that U.K. has a number of election pilots underway that do not use paper in their systems.

MR. KELSEY: Okay. It would be worth looking into that then.

DR. JEFFREY: Okay, thank you John. Are you up for a second or anything?

MR. KELSEY: Yes.

DR. JEFFREY: Okay, you are still up then.

MR. KELSEY: If you could just leave the slides the

way they first start I think it will be easier to use this.

In the last talk I was telling you about research we have done and trying to figure out how to write IDV standards. In this talk I'm really talking about our approach to writing security standards generally.

The goal we have, this is a broad approach about writing security standards and maybe it addresses some of the comments you had earlier in the discussion. What we are trying to do is write a standard that leads to secure voting systems. That means we need to understand how the voting systems work, voting system architectures, we need to understand the security requirements. We need to understand how somebody might violate the security requirements, the threat, the attacks.

Our threat analysis, our understanding of the attacks is really driving a lot of our writing of these standards. Once we understand the kinds of attack that are possible on our voting systems, we want to make sure we write requirements that block those attacks and make sure that those requirements are actually testable. Its not enough to say the system shall be secure you actually have to say how.

Lets just kind of look at the big picture and talk a little bit about how we are trying to do this. A sort of road map here is we need to understand the attackers and their goals and then we understand the threats to voting systems. We then figure out how to write a standard that addresses the threats.

The first part of this is understanding the attackers, what their goals are, what their resources are and how they might accomplish their goal. How they might do bad things to us. That gives us sort of a notion of the threats to the systems.

Then we are going to talk about determining defenses and how to write requirements that actually make sure those defense work. Broadly, current voting system architectures include, sort of, the optical scan systems, either hand marked ballot or machine marked ballot, the DRE with VVPAT, some sort of paper trial and the DRE without VVPAT. There may be other specialized categories but I think this kind of captures what's on the market.

You think about threats. You think about for each voting system architecture you try to identify what the threats are. What bad thing somebody could do to you. How could

somebody attack your system. You then try to figure out how to block those whole classes of attack or whole classes of threat to your system.

Blocking can either be prevention or detection. Prevention is like a padlock. Think of a ballot box with ballots in it. You want to prevent ballot stuffing. A padlock is a way of trying to prevent attacks. You try to keep somebody from getting at the ballot box in the first place.

Tamper tape or tamper seal is an example of trying to detect the attack. If somebody opens the ballot box later you look at the tamper tape an know this has been broken, something bad has happened.

Ideally you would like to prevent the attacks but if you can't prevent them, you at least want to detect them.

What are the attackers goals? Before you can start talking about security or anything you have to know what you are securing. The first goal that everybody understands changing the outcome of the election. That's like the critical thing we are worried about. We don't want to let that happen. That's where we spend most of our analysis.

It is also important to think of attacks that defeat the ballot secrecy. We'll find out how you voted.

Attacks that disrupt the election and by disrupting I don't just mean like a little annoyance, I mean causing the election to just shut down or having to rerun or having to be thrown to the courts or some horrible thing.

Those are all attacks that you want to make sure don't happen. You want to write standards that prevent those from happening to the extent that we can.

The threat methodology is kind of fun and this is really stolen largely from the Brennan Center's work. It is just really cool, really cool stuff that they were doing. The wrong question to ask is just can I tamper with a civic voting machine? That doesn't tell you enough to know if there is a threat.

The right question is can you tamper with the whole election? This is sort of the backward, the converse of Dr. Benalow's (sic) quote. You want to verify the whole election, not just the system. You want to know, can I actually defeat the election, can I tamper with the whole election, not just can I twiddle with one machine or one ballot box or something.

The approach here that the Brennan Center used and we have followed in our own analysis is start out by considering

a close statewide election, something that is maybe two percent or something. Its plausible that an attack actually could change the result. You might not know this.

You look for ways to tamper with the outcome. Try to come up with attacks that would change the outcome. Parameters like how many voting machines there are and how many voters there are in the state, how the counties are broken up, that actually turns out to matter quite a bit when you are doing this analysis.

Another thing that matters and that we consider is procedural defenses. You can look at, you know, if somebody is using say DRE with VVPAT and they are hand recounting one percent of their ballots versus if they are not hand recounting them, those are kind of different systems in some sense. The attacks look really different for those.

We kind of follow the Brennan Center's trick of evaluating attacks based on attack team size. How many people had to be in on the attack? The value of doing it that way is mostly that this is a parameter you can add. You can get numbers from different parts of the attack and add them together.

There are some problems with doing that in the sense

that sometimes you assume, you know, you hava a small conspiracy size that has these three specific people or something. This is, I think, the best way to consider how serious the attack are. The intuition here is that an attack that requires only five people in on the attack is much more serious than one that requires one hundred people.

How do we know about these threats? We are going to try to evaluate them. How do we know about this? There are a lot of sources. At the most basic level there's history and kind of folklore, stories that are going around among the voting community. You talk to election officials, you talk to people who have been in the voting world for a long time and they often know about bad things that either people did or people tried or that people worried about.

The Harris book was written in 1934 that talks about a lot of attacks. Some things still work or still apply. That's one source of information. What's been done before or what have people worried about in the field.

Another thing that we have to worry about is kind of current information on computer attacks. Voting systems have become more and more computerized, such as we're moving to the DREs and that means that a lot of the information

we need about how to attack those systems comes from the computer security world.

How are the commercial systems being attacked? How are banking systems being attacked or content protection systems or whatever? There is a huge amount of information out there from practitioners in the field and from academic literature of computer security.

What are the attacks we are seeing in the field? How are they done? What are the resources and stuff? That gives a lot of information on what's possible. What are the plausible attacks? How skilled might our attackers actually be? Maybe we can say, well, we know that computer criminals in other areas have this set of skills and this sort of resources, so we should assume that they might show up in voting too.

Once we start with those we have some very nice specific analyses of voting system components. Specifically usually voting machines but sometimes also the tabulation center software. The Hopkins report, the Robber (sic) report, Harry Hirstee's (sic) stuff, the Princeton report, Compuware (sic), a bunch of others.

Basically these are looking at specific pieces of the

voting system and analyzing them. Of course, the failing here is that often you find out there's an attack that works in the lab, you don't yet know if it works in the field. You can't just assume it doesn't but you don't know until you do the analysis.

The strength here is you find out a lot of ways that these systems fail. You learn something about the effectiveness of the testing system, the testing labs and the existing standards. When you look at a system that had a security failure and you say, well, why did it get through? Why did it fail? Is it that the standard didn't require the right things? Is it that the testing lab didn't catch a problem? What happened? That's a really nice source of information about attacks and threats.

Finally you get these analyses of the whole voting systems with procedures. We ran a threats workshop a year ago. It was like a year ago. We basically got a lot of input from the community, from a lot of academics and a lot of voting people on how these voting systems might be attacked. What the threats were.

The Brennan Center did this wonderful work on trying to characterize these attacks and put them into a framework,

you know, and its not perfect but they actually tried to put it into kind of a consistent framework where you could kind of look at it and do further analysis. That was really nice.

We also ran a workshop with George Washington University that also talked about threats. So its another place you get whole system sort of attacks.

That the source of the information about the threats, so at this point I just wanted to kind of show you that we have thought about the threats. We've done a lot of analysis. There a document in here on the security architecture that has a fair bit of discussion of the threats on existing systems that you can look at.

Now I want to kind of change gears and say once we know something about the threats. Once we know what we need to defend against, how do we defend it? How do we write the standards to do some decent job of defending it? So this is the second part of our road map. We are going to determine the defenses and make sure that we can actually require things that get them to happen.

For a lot of threats there are just kind of standard bits of computer security technology you can apply. If you

are worried about somebody tampering with electronic records in transit you can use digital signatures. Its well understood technology. Its been out there for a while. Its not impossible. Its not like there is any magic there. A lot of other things like control the software distribution, you know, assigning the software distribution, access control to make sure that not just anybody can walk up and do whatever they want on the voting machine. Requirements on event logs and configuration management and being able to verify what software is on the system.

All of this is fairly straightforward. The nice thing about those is you can require them and you can have the test lab just check whether they are there or not. You get a lot of value just by saying are you actually signing these records.

The kind of critical thing you find, not from looking at the components but from looking at the whole system attack, the stuff like the Brennan Center did, is the procedural defenses are so critical. That's not news to any of you guys who actually run elections but as a computer person I'm kind of like, wow, the people are really important.

For example, if you are worried, a huge number of threats

that you care about are blocked by a procedural defense. So, you think of something like tampering with the scanner software in a precinct kind of optical scan system. They might tamper with the scanner software.

So, you would like to make that hard to do but what if it happens. How would you detect it? If you are doing a random audit of just a few precincts you will like catch that if it's a wide spread attack.

You can actually work out the numbers for how many you have to do. That's not hard. We've got some of that in the document. So, you have a threat that you can't really address with technology but you can address the procedural defense.

Kind of the interesting question is, we're writing an equipment standard so how do we get some discussion of procedural defenses in there? We can't actually tell election officials what to do. Even if we could we wouldn't know enough because there is such a wide variance in counties running elections. We would know enough to give them exactly what they had to do.

What we do is, we can require equipment to support the procedures that we know are necessary for security. For

example, if you have DRE with VVPAT, its required, we can require that the VVPAT, the paper trail actually supports random, hand recounting that its not impossible to hand recount this.

Basically this lead to specific hardware and software requirements that come about to make sure that the procedure is possible and also that the procedure actually does what you think its going to do in terms of security.

Also this leads to documentation requirements. So the user documentation for the election officials have to say how to carry out the required procedures and the test lab has to check that to make sure that if you follow those directions you actually get what you are supposed to get.

Finally, there has got to be some technical documentation for the testing lab so that they can see why the procedure actually does what its supposed to do.

To give an example that is actually one of the harder ones to get right is parallel testing. If you've heard about parallel testing, this is testing on election day. The idea is you are trying to find out if there is some subtle attack program in your voting machines that is going to evade all your other testing and kind of become active on election

day and change the results on election day.

So what you do broadly is you isolate some randomly selected voting machines and you just run all day tests on them on election day. The goal is to make sure that those voting machines even if they are running some malevolent software can never find out they are being tested.

If they can figure out that they are being tested of course they will act right, they won't do the bad thing. This is a procedural defense against software tampering.

At first glance this doesn't look like it would have a lot to do with equipment requirements, but it turns out that it does. This requirement that the voting machine must never find out its in the testing environment actually means, for example, it can't ever be able to receive signals from other systems during the election. If it could, if the voting machine could normally be receiving signals from other machines, in the election then that would be a possible path for some other machine to warn that its being tested or for some person to come in and send a signal it being tested.

It pretty much can't be on a network during the actual election because then you would have to take it off the network to test it. There really can't be any observable

change from the voting machine that can detect that its in a different environment now that its being tested than it would have been just for voting.

These wind up giving you specific equipment requirements. If you want to support parallel testing, you have to impose the extra equipment requirements that are not obvious. Just to make sure that the procedure can actually do what it is supposed to do.

There are also other requirements that follow out of that like making sure that the documentation explains how to carry out a parallel test. It is important, for example, that you don't say, that you don't have a fixed number of votes or a fixed script that you always follow or something for every parallel test. If you did it would be easy to detect.

There is also the testing lab. VSTL is what we are calling the testing lab. It has to verify that documentation gives you good guidance, that if you follow it you actually get a real parallel test. In open ended testing, open end testing we haven't talked a lot about but this is sort of the opportunity of the voting system test lab to actually look for vulnerabilities, look for ways that even though

you've met the check list requirements, that you still fail to deliver on security.

So, in open ended testing one of the ways they can find that you failed to deliver on security is by finding a way for the voting machine to find out that it is being parallel tested when you follow the procedures that are given.

Obviously we can't go through a huge number of these examples but you can kind of see that the requirements, how we do the requirements, how we imagine these voting systems or envision these voting systems as being approved. First there is some sort of checklist requirements. If you require to use digital signatures, you actually can check that the digital signature is actually being done.

Then there's the documentation requirement where you review the documentation to make sure it fits the requirements.

Kind of the last bit of this is the open ended testing where you are trying to actually find the vulnerabilities. Hopefully those three approaches are different enough that we might find vulnerabilities from the last step that we didn't block with the first ones.

That's the overview of how we are approaching this and

how we are trying to write these requirements. We are basing this heavily on threat analysis, on understanding the attacks that can happen to these voting systems and then trying to make sure that they can't happen if you follow the standard or at least that they are harder. Of course, you can't every really block attacks one hundred percent. You really just make them more difficult.

A big part of this is trying to incorporate procedural requirements into an equipment standard in a way that makes sense and this is a lot of what we are working on. Also, this idea of equipment standards, documentation and open ended testing kind of overlapping to try to detect or prevent problems from coming out. Make sure that the final results is a secure system. That's it. Thanks.

DR. JEFFREY: Is there any questions or comments for John?

MR. BERGER: John I appreciate your presentation. I want to ask one question. When you are talking about the support for parallel monitor testing, did I understand right that the kind of system clock would be very important to that?

MR. KELSEY: I'm sorry, the kind of system clock?

MR. BERGER: The kind of system clock. In other words, that the system if you wanted to maximally support that kind of testing, the clock should not tell the system what day of the month it is, it should be relative to the start of an election so that in testing you could then start and the machine would see exactly the same thing it would on election day.

MR. KELSEY: Right. That's a different way of accomplishing a similar requirement. In some systems people will try to make the voting system, you know, stateless, make sure that it can't know whether, it can't know what's come before, or what will come after. Its sort of a variation of that.

So, if you did what you are talking about what would happen is you would have, you would be able to run the parallel test three weeks earlier or something and still have the same result. That isn't in our current requirements although that's a reasonable thing to think about.

MR. BERGER: Let me ask against the current class of voting systems how amenable are they to parallel monitor testing?

MR. KELSEY: I haven't looked into the current voting

systems in great depth. I know there are quite a few that have some sort of networking connection and I believe the bigger issue and maybe I can back up on this because I think I listed this. The bigger issue for parallel testing, apparently I didn't include that --. There is usually someway that you get authorized to vote.

Somebody might give you a smart card, for example. They might give you a three digit number, four digit number or something to authorize you to go to the voting machine and vote. That actually is a place where often you have a system that is communicating with the voting machine or you may have a pool of ten or fifteen smart cards or twenty or whatever, that are being circulated during the election. Those are things where you would have to either procedurally or in terms of the design change that to accommodate good parallel testing.

For example, if you have a machine that's talking to the voting machine all the time, you are going to have to disconnect it from the original judge's station and connect it to a different station to do your parallel testing and you have to convince yourself that can't ever be detected by the voting machine.

I haven't tried to go, I don't think any of us have tried to go and find in depth exactly which systems would comply with the standard we are trying to write. I think that would become, it would probably become an almost untenable amount of work to try to check that for all the requirements we are writing.

DR. JEFFREY: Any other comments or questions? Okay, thank you very much John. At this point I think I'm going to call for a lunch break, at least my stomach is growling, I don't know about the rest of yours.

For the TGDC members and the EAC representatives here we have a dining room reserved for us, A & B. For everyone else there is a great cafeteria and lots of restaurants around the area. I would suggest that we reconvene thirty minutes ahead of schedule so t 1:30. So, please plan to reconvene at 1:30. Thank you. (**LUNCH BREAK)**

DR. JEFFREY: If I could ask everyone to please take their seats. We are going to get started again in just a minute.

Again, if I could ask everyone to please take your seats so that we can get started.

Okay. Welcome back. We are going to continue the

discussion from the Securities and Transparency Subcommittee. There is a, I think one more briefing on this subject.

The parliamentarian has correct me. Roll call first to ensure that we've go a quorum.

MR. GREENE: This is a roll call for the afternoon session.. Williams.

MR. WILLIAMS: Here.

MR. GREENE: Williams is here. Berger.

MR. BERGER: Here.

MR. GREENE: Berger is here. Wagner.

MR. WAGNER: Here.

MR. GREENE: Wagner is here. P. Miller.

MS. P. MILLER: Here.

MR. GREENE: P. Miller is here. Gale. Gale not responding. Mason.

MS. MASON: Here.

MR. GREENE: Mason is here. Gannon.

MR. GANNON: Here.

MR. GREENE: Gannon is here. Pearce.

MR. PEARCE: Here.

MR. GREENE: Pearce is here. A. Miller.

MS. A. MILLER: Here.

MR. GREENE: A. Miller is here. Purcell.

MS. PURCELL: Here.

MR. GREENE: Purcell is here. Quesenbery.

MS. QUESENBERY: Here.

MR. GREENE: Quesenbery is here. Rivest.

MR. RIVEST: Here.

MR. GREENE: Rivest is here. Schutzer.

MR. SCHUTZER: Here.

MR. GREENE: Schutzer is here. Turner-Buie.

MS. TURNER-BUIE: Here.

MR. GREENE: Turner-Buie is here. Jeffrey.

DR. JEFFREY: Here.

MR. GREENE: Jeffrey is here. We do have a quorum. You may proceed.

MALE SPEAKER 14: Dr. Jeffrey may I just point out for new people who may have come in that we have signers over in stage left and if you would like to take their services, please come sit closer. Thank you.

DR. JEFFREY: Thank you very much. Again, welcome back. I hope everyone had a good lunch. I will now ask Nelson Hastings to come up and discuss update on 2007 security requirements. Nelson.

MR. HASTINGS: Is this on? Good afternoon. I'll give you a little update on what we are doing in the area of security requirements for the next iteration, I guess, if VVSG.

My presentation is going to take three parts, to give you kind of a status, overview of where parts of the security requirements are at right now. I'll talk a little bit about the approach that we are going to take in the 2007 VVSG towards wireless communications and look specifically – the third part of the presentation will look specifically at new and modified requirements related to voter verified paper records, securing electronic records and set up validations.

The status of security requirements. First, I'll just discuss the development process that we are using. We draft requirements based on research. We get input from vendor community, the election community, and securities community as well as looking at using the threat work that we have done as well as looking at previous versions of voting system standards. Once we draft those requirements, we distribute that within NIST. The NIST voting team will review those requirements and will update those requirements based on the comments that we receive.

At that point we distribute it out to the STS subcommittee for review. We update those requirements based on the comments that we receive and then we present it and ask the TGDC to review those requirements.

Right now what we have is, we have two white papers, one is an approach on how we are tying together all the different aspects of security and we also have another paper on open ended vulnerability testing approach. Those papers, specifically the open ended vulnerability testing approach is a very drafty, first stab at our approach that we are going to take and due to time constraints today we don't have time to go into that white paper in detail.

In addition, we have seven draft sections or seven topic areas relating to security requirements and that's what the draft white paper on how we tie things together, how we are going to bring those seven section together.

So, I'll start to go through the seven sections that we have right now and what state they are in. We have access control requirements. First of all the topic area here that are up here, access control, cryptography, set up validations, software distribution and installation, have been converted into the requirement format, the final format requirement

for VVSG 2007, just as a step in the process.

We have access control which has been presented in March of this year and that hasn't really changed since that was presented. Those requirements really haven't changed.

The cryptography section has been presented in March of this year as well. That part of the requirements related specifically to key management and is being rewritten and updated. I'll talk a little bit more about that in the presentation on securing electronic records and you will see why those cryptography requirements need to be updated.

The draft set of validation requirements, that has been developed based on 2005 set of validation requirements. I'll talk a little bit about that also later in the third part of the presentation and those requirements are in a state of, we've circulated those among the STS subcommittee and have received comments back on that. We are in the process of incorporating those comments.

The software distribution and installation requirements are based on the software distribution and installation requirements of 2005 as well. We have updated those as well. They are in the process of going through the NIST internal review and once that process is done we

will distribute that to the STS subcommittee for comment.

Then we have the system event logging requirements and those are also being converted into the 2007 format. They have been through the NIST, they are in the process of going through the NIST internal review. That's a completely new section that's being developed. Its grabbing some requirements from the old VVSG 2005 as well.

Also, the last two items on the list here are the physical security requirements and the system integrity. Management requirements those are very drafty. They haven't even been, the requirements haven't even been drafted and converted into the VVSG final format. So, that stuff is still in the development, very developmental stage and it hasn't even gone through the NIST internal review yet.

So, what are we going to do? We are going to continue to create draft requirements specifically in those last two areas. We will continue to circulate the draft requirements for review as they become mature enough to do that and modify and refine the requirements based on the comments that we receive.

Right now the seven sections are not incorporated into the VVSG overall document at this point so what we have to

do is we have to integrate those sections in and harmonize with the other sections as needed. A specific example of that will be the documentation requirements that are strung through the different sections. We need to collect those in th appropriate section of the overall document.

Now we will talk a little bit about our approach to wireless communications. This talk is based on the white paper that was in your package, called "The Draft White Paper on Wireless Issues in STS Recommendations to the TGDC." To give you a little context, the VVSG 2005 really defines wireless communications as any communication that travels over the air or through the air.

There was no recognition in VVSG 2005 on the different levels of difficulty needed to secure the different types of wireless technologies. What we would like to do is take and look at wireless technologies in terms and focusing it on infrared technologies and radio frequency type technologies.

The first thing we did, is we looked out and say and asked the vendor community how they are using wireless technology in their voting systems. RF and IR technologies are being used to install software on voting equipment.

RF technologies is being used in the transmission of unofficial results. That technology is being used in the form of cell phones and that kind of thing.

Signaling, opening and closing of the polls, that functionality is being done, in some cases, with radio frequency type technology as well as collection of cast ballots after the polls close, collecting those and consolidating those at a polling place is being done with IR technology.

We have also seen wireless technology in terms of T-coil for hand sets or head sets and ballot activation is being done using IR technology.

So what are some of the issues with wireless communications? The wireless signals can be intercepted, inserted or disrupted. This leads to reliability issues. If you rely on wireless, the wireless capability to perform a function. VVSG 2005 actually acknowledges that by requiring that any capability or functionality that a voting system has that relies on wireless technology requires a back up method that does not use that wireless capability if it were to fail.

Technology to attack wireless, specifically radio

frequency signals, easily obtained on the internet and things like this, hacker sites and whatnot. The platforms that are used to launch such types of attacks can be easily hidden such as small portable devices such as cell phones and PDAs.

Some other things is that the security measures for wireless communications are complicated to configure. Its hard to configure wireless devices securely. We have trouble doing that even as security experts of getting that right.

Lack of maturity of the security countermeasures for wireless technology and by having wireless technology in the voting system, it creates a path for an attack that we must acknowledge and defend against.

The STS recommendations are to allow IR wireless communications but restricted as per the VVSG 2005 which basically means that the line of sight path that's used needs to be shielded and protected as well as the signals need to be authenticated and encrypted as they are traveling through the air.

For RF, wireless communications, STS is recommending that wireless LANS and other RF not be permitted to voting equipment. Specifically voting equipment that captures

casts ballots. So that would be 80211 type wireless LANS and those kinds of things.

A separate communication device could be used to transmit unofficial results using RF wireless technology but that device would have to be a piece of voting equipment that doesn't actually capture voter cast ballots.

So, what's the impact of these recommendations on the use of wireless as we see it in the field? As far as T-coil technology goes there is no impact. As far as the installation of software using radio frequency type networks that would be eliminated and you could only install software using IR technologies.

In transmission of unofficial election results we require separate communications device. Again, a device that doesn't capture cast ballot votes. The collection of cast ballots after the polls close that would be prohibited. Prohibited here means prohibited in terms of the use of radio frequency technologies. The same goes for signaling the opening and closing of polls. These would be prohibited using radio frequency. You could do that if it was implemented using IR type technology. Those prohibited kind of have some caveats to them.

We would have to upgrade the IR communications as per VVSG. Like I said you could still continue to install or load software and activate ballots based on that. At this point I am sure there is much discussion to be had.

MR. SCHUTZER: So, if I understand what you are saying, the recommendation is to just not have any kind of resolution, just leave it the way it is in the current 2005, is that what you are saying?

MR. HASTINGS: I think the current 2005 is my understanding. You can correct me, and you can correct me back here as well, is that it allows both radio frequency as well as IR technologies. Radio frequency technology can be used for any –

MR. SCHUTZER: I thought you said it was keep the restrictions that are currently in 2005.

MR. HASTINGS: That's only specifically to the use of IR technology.

MR. SCHUTZER: Oh, okay.

PROFESSOR RIVEST: We do have a resolution from the STS subcommittee which straightens the wireless along these lines which I can read at an appropriate time here.

MR. WILLIAMS: I have a question. Why are you concerned

about the transmission of unofficial results?

MR. HASTINGS: Its allowed with RF when you use a separate device that doesn't capture.

MR. WILLIAMS: Same question. Why are you concerned about that?

MR. HASTINGS: What we are doing by having a separate device is we are providing an air gap between the voting system and the device that's used to actually transmit the unofficial results. What we are doing by doing that, providing that air gap, is it doesn't provide a wireless capability into the voting system directly. That's why we have this separation of two devices.

MR. BERGER: I'm curious. The recommendation to not allow RF in voting equipment that captures the cast vote ballots, what was your discussion about having a similar prohibition on the equipment that accumulates the votes?

MR. HASTINGS: You mean at the back end?

MR. BERGER: Well, first of all, is the implication that RF devices would be allowed on the election management systems or would that also be prohibited?

PROFESSOR RIVEST: The Resolution I could read would help clarify it. It does talk about systems that

(undecipherable). Should I?

DR. JEFFREY: Yes, why don't you please enter it.

PROFESSOR RIVEST: So let me do the resolution. Maybe just of preface it by a more direct answer to your question which is that the wireless would be disallowed in systems that have counting capabilities as well, counting functionality for the system.

Let me read the resolution into the record and then we can debate it extent or what we desire for its extent.

Here's the proposed Resolution: "The TGDC has considered additional security research since Resolution #35-05 was passed and has concluded that the presence of or capability for any wireless in equipment whose purpose is for official vote casting, counting and reporting should be prohibited in the next iteration of the VVSG. The sole exception is for infrared wireless, which should only be allowed if the physical path is shielded in addition to the security measures already in VVSG 2005."

So wireless will be prohibited for official vote casting, counting and reporting.

DR. JEFFREY: Are there any other questions or comments? There is a resolution now on the table. So any

discussion on the Resolution as well as questions?

MR. WILLIAMS: This is Brett Williams again. I guess I've got a concern here. We talk about usability and ease of use and if you are dealing with say, a DS&S or a Diebold DRE, and you've got to prepared memory cards and you are a county the size of Fulton County, you got to prepare three thousand memory cards and keep them separated by precinct and all.

Its quite a logistic effort whereas with some certain wireless systems you can sit at a console in your warehouse, where the warehouse is shielded and program those three thousand voting stations from that wireless station.

So, we are giving up something here, okay. The question is are we, is what we're giving up worth what we are gaining? Has there been any instances of this actually being exploited?

PROFESSOR RIVEST: Great question. I have a couple of answers to that. First, use of wireless for the kind of purpose you are talking about today, doesn't seem to be very widespread. So, if you are asking about current exploits I would view this more as a preemptive measure rather than a reactive measure.

I think the distinction here would be between RF and IR. IR would be permitted to load the software in the fashion you are talking about because IR can be shielded. It's a line of sight. It can be shielded.

RF, there is no practical way to shield the building and so that's the basis behind the recommendation.

I don't know if that answers your question. If it doesn't please ask again.

MR. SCHUTZER: I have a question. It sort of goes like this. I know it didn't pass but if one had passed, the software independent verification. The main concern of threat of wireless is its an easy way to insert or modify some code on the voting machines. If you had the software independent verification, would you this concern still be there if one were using it as mentioned?

PROFESSOR RIVEST: Maybe I can speak to that. I think that's a great question, Dan, because if we had passed the software independent resolution it does relax the pressure on a lot of these other mechanisms we are talking about. Set up validation, you know, all the various mechanisms. It doesn't mean you want to eliminate them, I would say, but that may the rigor with which you need to apply them

is reduced.

Given that we haven’t passed it, I have concern about how high we need to raise the fence on some of these. We need to talk about those things. Great question.

MR. WILLIAMS: Are you saying, Ron, that if we had passed that other resolution, you would have withdrawn this one?

PROFESSOR RIVEST: No, I wasn’t saying that, but I would feel less motivated for this one, definitely.

DR. JEFFREY: Any other comments on this Resolution or questions for Nelson? There is a resolution proposed, is there a second?

Okay, its been proposed and there is a second. Let me see, is there a question for a unanimous consent?

Any objections to unanimous consent?

No objections. By unanimous consent this Resolution passes.

MR. HASTINGS: So now we will talk a little bit about the new and modified requirements specifically in verified voter paper records, securing electronic records and set up validation.

We will start off with voter verified paper records.

This presentation is based on the white paper VVPR Issues and STS Recommendations for the TGDC. The voter verified paper records support the ability to perform independent audits, you know, op-scan, VVPAT and the electronic ballot marking devices and electronic ballot printing devices as well.

In VVSG 2005 the requirements really centered around voter verified paper audit trials. What we would like to do in 2007 iteration is to address all paper type records or voter verified paper type records. The goal is to ease the use by the voter and poll workers and make it easy to audit those paper records.

We previously have had a lot of debate in previous TGDC meetings on specific implementation, specifically related to paper rolls and bar codes and we will talk a little bit about that here. There are a lot of issues, pros and cons, related to paper rolls. I've only written down one or two of them for this presentation.

One the pros is that it is difficult to add or remove a cast ballot or an audit record that is on a paper roll, that instantiated (sic) in a paper roll. However, there is cons to that as well. Potential violation of privacy

and some usability and accessibility issues. What the STS is recommending is to allow paper rolls but to improve their security and usability.

MR. SCHUTZER: I think there would probably be another kind too. I mean if I ran out of paper rolls, or then I might have some difficulty running to like the neighborhood store to sort of buy more paper rolls. If I had just normal stock paper, I would probably be able to get up and running in a relatively short period of time.

MR. HASTINGS: I acknowledge that I haven't exhausted the list of cons here, I just kind of give it flavor here.

MR. WILLIAMS: Could you be a little more specific with what you mean by improved security and usability?

MR. HASTINGS: Ron, would you address this?

PROFESSOR RIVEST: The improved security basically it seems like the big trap people complain about is that someone could actually look at the paper roll and see the order in which people voted.

It seems that if its possible to make the housings such that they clamp shut and it would be evident to anybody at election headquarters whether they were opened up after being removed from the machine then at least, well I guess what

I'm trying to say is the violation of privacy is more likely to occur at the polling place than I think it would once it gets into election headquarters.

So, the idea at that point is basically make it evident if there has been any opening of the paper roll housing, some sort of mechanism to do that.

The usability. Well, usability, this part of the talk could go on for quite a long time. Its fairly basic stuff. Its just, you know, basically including some tools to actually deal with paper rolls.

Election officials should not have to get a big long table and scroll them open. They ought to have some mechanical aids for dealing with them.

Usability may also extend to making sure that the software used to actually configure the information that gets printed on the paper rolls is easy to use and works reliably. For example, if you have a multi-precinct polling site and you have the same VVPAT systems used for, in essence multiple elections, at a minimum you want information printed on the paper records for each ballot basically indicating which election it was used for, so that you can at least audit with some precision at that point.

The software in the documentation for printing out those reports has to be easy to use and well understood. Election officials have to be able to use it readily and come up with the proper configuration. So it extends to the information on their as well.

Just another thing too is that if you have to use multiple paper rolls, of course, they have to be very easy to put in and take out. Election officials, well, I should say poll workers, end up be system administrators.

The equipment has to be reliable and it has to be usable. When you tear off the paper roll, it should not cause the paper to accordion. All that stuff can be fixed and it can be fixed easily. We know how to do that. So, those are all the sorts of things we are saying basically.

MR. WILLIAMS: What about the printer itself? Are you addressing that? Right now most of these implementations were thermal printers which are probably the worst printer on the market.

PROFESSOR RIVEST: Well, we've worked with printer people at NIST and talked with others and we have higher reliability requirements for that equipment. Our conclusions are that thermal printers but higher quality

thermal printers with thicker paper would actually prove a lot more useful. It appears that the paper rolls used today have some of the thinnest paper and the printers in general are not of the highest quality. So, yes.

MR. SCHUTZER: You know we are just talking about it for 2007 so we are not talking about impacting that which was done in 2005 and it may be naive but it just seems to me that if one were to talk about the stock printers that you have these days take normal paper, normal ink cartridges, don't have the problem of having to put in rolls, when they go down you could do any kind of variety of things in terms of sorting them in some random manner, I'd almost be inclined to say that I wouldn't recommend paper rolls for the future.

PROFESSOR RIVEST: Well, we have somewhat difficult to parse language in that paper. The STS conclusions here were to permit it in VVSG 2007 but to include a should requirement or some statement that effectively signals that its not the best approach and vendors should go in a different direction. Paper rolls just has the inherent violation of privacy.

So we are including, you know, basically the capability to still use them. There are many advantages. One advantage

would be that existing VVPAT systems would still be certified to the 2007 standards, but some signal that says better technology should be used.

MALE SPEAKER 15: I like to ask a follow-up question. You've kind of put it on the table there that, I mean, I guess the TGDC could tell us not to pursue paper rolls anymore in our development of VVSG 2007. Is that what you are suggestion?

MR. SCHUTZER: That's what I was suggesting. I don't know how other people feel. The printers are more common and more reliable. The paper is more reliable. You probably have less trouble managing it. You would avoid a lot of the privacy issues. Its easier to load and unload.

It would have to be appropriately designed with some kind of closure so people couldn't pull it out. Its not exactly off the shelf but that would be my inclination.

MALE SPEAKER 16: Are you making an official resolution?

MR. SCHUTZER: Sure. I'll make a resolution that in 2007 one not recommend paper rolls but recommend the more discrete papers. I don't know the proper wording for that, if someone could help me out?

MALE SPEAKER 16: If you are looking for an outright prohibition, you need stronger than not recommend.

MR. WILLIAMS: I wouldn't go that far. I would charge the STS committee to investigate this further rather than make it an out and out prohibition. I don't think we even need a resolution for that do we Ron?

This paper roll has been controversial from the get go. When it was first proposed by Nevada, you know Nevada got out front and bought the things before they ever got approved and it became a political hot potato and its been controversial from the get go. I would like to see a real thorough vetting of this issue.

PROFESSOR RIVEST: We can look at it more certainly within STS but I think its really this committee that's got to make the hard choices somewhere.

MS. QUESENBERY: It seems to me this is a place where the intersection of STS and CRT requirements is really an issue. Certainly on HFP our predilection has been to try to write results requirements rather than actual design requirements.

Let me try to say this so it doesn't get misquoted. If, in fact, we think that cheap thermal printers don't have

a high enough reliability, then it should be covered by reliability requirements, not by banning thermal printers.

It might be something that the two committees ought to work together on to make sure that the CRT requirements are sufficiently strong and are specifically addressed. We do this in HFP where we started with accessibility requirements in the VVPAT section and made sure that the two sections coordinated properly.

PROFESSOR RIVEST: There is the privacy issue as well. We need to balance that as Nelson said. There is a trade off between procedural issues and how severe the risk is and I think this committee has got to decide that in the end but we can look at it some more.

MR. SCHUTZER: But in this case if you had separate pieces of paper you'd (undecipherable) from the privacy issue to. You could almost consider like a random sorting –

PROFESSOR RIVEST: No, I like the separate pieces of paper idea. I wish we had more evidence of that approach on the market.

DR. JEFFREY: Okay to summarize the discussion, (undecipherable) we have disagreed on is that the STS is being tasked to investigate this issue further with an eye

towards perhaps performance based standards as opposed to design based standards and to look at all the issues including the reliability and the privacy. So, that's sort of the intent of the committee without a formal resolution.

MR. WILLIAMS: Basically what we are saying is take that last sentence that says improve security and usability and see if you can expand that into something that's defensible.

MR. HASTINGS: Another issue has been the issue of bar codes and again there are lots of pros and cons to that and I've only written down one here for each one of those.

One of the pros is that it helps making scanning paper simpler for election officials. The con is that the voter cannot verify the contents of that bar code itself. Again, STS is making a recommendation to allow bar codes.

However, the audit procedure associated with those paper records must not depend on that bar code being accurate.

MR. SCHUTZER: Well, we are laughing because --. So what you are saying that in case of an audit, you couldn't rely upon the bar code. You can't use the bar codes to do an independent audit because the bar codes might not match what the user saw.

MR. HASTINGS: Right.

MR. SCHUTZER: So, in essence, the question is why bother with the bar codes then?

MR. HASTINGS: Okay.

MALE SPEAKER 16: Or you can't use the bar codes alone.

MR. HASTINGS: Right. I think that would be more –

MALE SPEAKER 16: But you could scan the bar code and visually confirm that it matches.

MALE SPEAKER 17: What does that buy you?

FEMALE SPEAKER 6: More time auditing?

MR. HASTINGS: So should I ask the question again?

MR. WILLIAMS: Some of us have thought this was all kind of almost a joke on this ourselves because you are saying that I don't trust this computer that wrote that bar code but I got one over here that's going to count them and I trust it.

MR. GANNON: Nelson, would you clarify, are you talking about bar coding of the entire contents, identity as well as the actual ballot information? Are you talking about just bar codes used to identify which race, which election, which precinct, etc.

MR. HASTINGS: John, I need help here again.

MALE SPEAKER 18: We did not put a restriction. We talked about it but we didn't put a restriction in there. The way we ended up going with the requirements, writing it out was essentially that not so much allowing a bar code, but if any information on the paper record is encoded so as to assist in making it machine readable, then, you know, various requirements around that. That's pretty much the way we have it.

Would you recommend, are you recommend that the ballot choice information not be encodable?

MALE SPEAKER 19: Yes, I think that's the situation we are looking at is the sensitive information that you want to be sure is human readable. Certainly the ballot information, the information identifying the race, precinct, etc. might be bar coded as well as printed so that you can machine sort, etc.

PROFESSOR RIVEST: The dilemma we had was that in some states where there has to be a recount and the paper roll, the bar code issue really came up with paper rolls more than flat cut sheets of paper.

If there is a recount and, you know, you say to a bunch

of election officials to recount all these paper rolls, they are going to be unhappy. At that point having some capability to scan it in, would be much more helpful.

I do want to point out that in your routine one percent audit, no you could not use the bar code. You would have to establish that the bar code does match the human readable content, but in the case of recounting, its seems as if providing the option of having it would be very valuable. Maybe some states that would recount the paper might want to use that option. States that don't maybe wouldn't want to use that option.

MR. SCHUTZER: Here's my take on what I think I'm hearing and my thoughts on it.

I think what im' hearing is that certain things might be very valuable to encode because it might help. I have a whole collection of ballots and now I want to recount in a selected part of it and I could just sort of, you know, spin out the ones that I want to count manually that way. That's what I hear.

That, at first, sounded appealing to me. I thought about that and I said, you know, if I were attempting to do something with an election what would prevent me from

modifying all the bar codes to read one or the other even though, and I'm saying you just won't get all the ones that I modified, you just get the ones I choose to have you recount if you were to use that bar code marking.

PROFESSOR RIVEST: We had a number of discussions and I think one of the conclusions we can to was that the bar code, the existence of the bar code is a little bit more tied to the use of paper rolls than it is to flat cut sheets of paper which are more reliably optically scanned. Yeah, it is a significant attack vector but at the same time it would be very difficult for a state to have to manually recount many paper rolls.

It is a dilemma and we didn't have a good answer. We tried to err on the side of doing no harm.

PAUL MILLER: Couldn't there be audits that are sort of a combined use audit. You do your one percent manually. Certainly you would have to do part of your audit manually. If you wanted to do a four percent audit or a five, or six percent audit couldn't you authentic the bar codes by doing your one percent audit and then use the bar code for the larger audit?

PROFESSOR RIVEST: David could probably answer it

better than me.

DAVID WAGNER: This is a complicated subject. Bar codes are tricky to use for the purpose of audits. There may be some cases where you could use them. I think its going to depend heavily on the purpose of the audit.

If the reason why you wanted to do a four percent audit instead of a one percent audit is to get a higher degree of statistical confidence that the voter verified records matched the electronic records, then you need to be doing it manually.

On the other hand if you are doing the audit for some other purpose, if the failure mode you are worried about is not a mismatch between the electronic and the paper records but some other kind of failure mode, then you may indeed be able to do exactly as you say, use the bar code --- Establish the accuracy of the bar codes using some statistical measure and then count the larger number of the bar codes. Its possible.

MR. SCHUTZER: So what I'm hearing now is that in addition to all the other negatives for the thermal roll I'm hearing that it even has trouble with some of the standard optical character recognition that would preclude the use

of optical character that is used very successfully to see a little number for the election district and everything else.

It sort of says to me, you know, if it jams more easily. If its harder to get supplies. If it can't do optical character reading right. If it doesn't do the privacy. Then why am I entertaining keeping it for 2007? I don't see it.

MR. WILLIAMS: You left out one. It just took us a solid man year to count the rolls off of six voting stations.

MS. QUESENBERY: How did we get back to rolls?

MR. SCHUTZER: Because we just heard the whole purpose of the bar code was to compensate for the fact that the rolls can't produce characters of sufficient precision that standard optical character recognition could do it. In today's day and age I could do the same sorting and finding it out by precinct by just having the right kind of codes in the corner of a normal piece of paper with a normal ink jet printer.

MS. QUESENBERY: The thing I was going to say, and I'm sorry its not completely gotten through is that the advantage of something that's machine readable, whether it's

a bar code or some other sort of code is that it can make it possible to read back a piece of paper, scan it and read it back through headsets. So, it can increase accessibility.

Having said that, a more desirable solution would be to have something that could actually read the text, actually read the unencoded ballot. Those are beginning to come on the market.

Just not to lose sight of the fact that something that renders information machine readable, has some advantages.

MR. SCHUTZER: So we are saying also that if you were to have something of this quality, it probably be on a machine that could read it to somebody.

I'm almost inclined to put a resolution on and not waste anybody's time.

DR. JEFFREY: We're open to resolutions but unless the resolution comes forward, then we would still be at the point of.

MR. SCHUTZER: I'll throw it then. I resolve that for 2007 we prohibit the roll paper.

MALE SPEAKER 20: I'm second.

DR. JEFFREY: Before the second let's discuss. Let's see, who has the electrons? Allan.

So, Dan, if you could actually phrase the actual resolution then we can tweak the wording.

MR. SCHUTZER: All right. I'll try my best. That the paper rolls for use in verifiable paper trial should be prohibited for the next iteration.

Please feel free to amend that wording.

DR. JEFFREY: I think he's amending it not necessarily intentionally.

MALE SPEAKER 20: Another wording might be continuous rolls shall not be used for VVPAT in –

MALE SPEAKER 21: So what came out of the line?

MALE SPEAKER 22: You get to see we are quite a committee here.

MALE SPEAKER 23: For use as a VVPAT.

DR. JEFFREY: Okay, so there is a resolution on the table for the discussion. Helen.

MS. PURCELL: Are we making any recommendations as to what will replace the paper rolls since we have a number of states out there who are already using it? What is our alternative?

MR. WAGNER: As I understood the obvious alternative would be cut sheet paper records. For instance, 81/2 x 11

individual sheets. One sheet per record.

MS. PURCELL: Again, which at this point are not designed yet so we are talking about something way in the future because we have nothing currently that I am aware of in any of our systems of that design.

MR. SCHUTZER: The DREs won't have ports, output ports?

MALE SPEAKER 24: Wasn't there one system that did have cut sheets?

MR. WILLIAMS: Yes, there is at least one system on the market now that has that and I'm aware of at least one other vendor that's going to add that capability to the DRE machines.

All of the existing ones are Rube Goldberg type of clutches so, this is not a high impact type of thing.

MS. QUESENBERY: Just to come back to what Commissioner Davidson said, this would be new machines not, and we are talking 2010 at this point.

MALE SPEAKER 25: With the next iteration.

MR. HASTINGS: I have a question on this one.

DR. JEFFREY: Nelson you may ask questions.

MR. HASTINGS: As its written right now, its talking about VVPATs specifically. In our discussion of voter

verified paper records, do we want it to be specific to VVPAT or these paper rolls I'm talking about now?

I guess what I'm trying to say is we are trying to generalize the discussion –

MR. SCHUTZER: It wouldn't affect optical scan balance. So, are you talking about ballot marking machines or things like that? Is that what you are referring to?

MS. QUESENBERY: Can I just make a suggest that we let someone go off and work on wording this and come back because doing the wording like this never produces a very great result.

MR. HASTINGS: Well, we have tomorrow afternoon I guess.

MS. QUESENBERY: Yeah, we could come back to this.

DR. JEFFREY: As long as there is no objection, I'll ask Nelson if he could take the lead on working on a revised version of this to present tomorrow or today if you are ready.

MR. GANNON: Before we dispense with this can I get a recap as to why we are trying to do away with this. I thought there was a need to have some voter verification and I understand that those issues of cost and readability but what I understood was being proposed was that there was

better mechanisms needed to deal with paper rolls.

MR. SCHUTZER: There is only two reasons in my mind why I would want to do this. Since we don't have anything on the horizon except for the innovation that provides the independent software verification one would like to at least improve upon the paper output to the greatest extent possible. Just about everything I see, you know, talks about the problems primarily being posed by the thermal rolls.

The other thing is we have precious little time, we have other resolutions we'd like to put up in terms of really studying the kinds of problems we've had in the current election and just reviewing the specifications and see what we can do to impact and minimize those kinds of problems in the future. I would rather have people devote their time and energy on that than to try to figure out how to make a thermal roll a little more secure and a little more maintainable, etc. It seems to fly in the face of efficiency of time and effort and resources and have people concentrate on that. So I would just as soon do away with people spending time on that.

PAUL MILLER: I'm not a big fan of paper rolls but I'm not confident that we have established – I know that

there is one or two vendors, Brit, who have the cut paper approach to the VVPAT but I'm not aware of any large scale implementation of those systems. I'm not aware that we really have demonstrated that there is a better alternative to the paper roll.

I am a big fan of the idea of us looking and studying whether or not there could be better implementations. Paper roll is not ideal, but I question whether or not we can just strike out the use of it at this time, whether or not we really have better technology available to us.

MR. WILLIAMS: About thirty or forty minutes ago that was our initial recommendation was that they go back and expand this security and usability clause.

MR. WAGNER: We can leave it at that. If you would like a recap I can recap for you without, you know, supporting one position or another. What I understand the pros and cons to be. Is that worth doing or would you rather that we table this for now.

The cons as I understand it from the security point of view of the continuous paper rolls so there's the privacy concern that they preserve the order in which voters vote. I think there are some non-security related concerns that

we've heard.

We've heard the reliability concern. We've also heard the usability issues for election officials that they may require mechanical tools for audit. They may be difficult to recount.

In addition, I have heard a concern raised about the usability the small size limits the amount of information that can be presented.

The pros of the continuous rolls as I understand them, if its all on one reel, the rolls may be easier to transport and to store and to manage. Another pro of the current system with the thermal printers is that they are relatively simple inkless devices so you don't have, for instance, ink to run out of. That may have some reliability benefits.

I don't know, I'm not an expert in reliability. I'm just repeating what my understanding of the arguments was.

The third big pro, the big argument for allowing them as I understand, which probably may be the strongest one, is that if paper rolls were allowed that would allow the existing systems which do produce paper rolls to be certified to the 2007 VVSG. That would have the advantage of preserving many options for election officials.

MR. SCHUTZER: If it was really a complicated thing but, you know, all of the voting machines are based upon off the shelf kinds of P.C. stuff. They all have drivers that drive all these common variety printers and without getting overly complicated assuming that each individual voter is not in collusion to modify his vote. One could see the piece of paper come out and a box with a slot in it and the voter looks at the piece of paper, verifies it, puts it in the slot, where it then can't be retrieved. I don't understand the – I mean I could think of a heck of a lot of other better ways of doing that but that certainly would allow somebody to almost immediately for not too much money be able to use this other method.

MALE SPEAKER 26: If I could add to David's list of cons too, things that were mentioned earlier. One was the difficulty of auditing the long rolls of paper tape and the second was the difficulty of using any kind of OCR.

DR. JEFFREY: I think at this point we've got that you will put together a draft resolution and it will be presented when its available.

Unless there is further discussion on this point we should move on.

MR. HASTINGS: Some additional STS recommendations in relationship to paper records is to require better documentation as well as tools that are used to audit the paper itself, you know, auditing software and that kind of thing.

We also wan to enhance reliability of printers and their associated mechanisms. That's an area of overlap with the CRT folks as well as look at the entire voting process for accessibility when paper is used in the voting process. That's an overlap with the HFP folks.

Now we are into securing electronic records. The goal of securing electronic records is to make sure that the records as they are being transferred from the voting equipment to the central tabulation equipment is secure. We want to prevent alteration or back dating of those records and we want to provide digitally signed cast ballots and totals to support canvassing.

In order to do this what we need to do is we need to fully specify the record formats and that's record formats for cast ballots, individual as well the composite of those cast ballot records, voting equipment total as well as system event logging records that are generated. These electronic

records would require, in addition to the information of the electronic record, information on software versions and configuration files, time stamps and digital signatures.

I will talk a little bit about how to get those digital signatures on the electronic records. The suggestion is to include hardware crypto modules in each voting system. The hardware module would be designed in the voting system to be permanently attached to that voting system. It would not be able to be removed. What this does is it helps to limit software attacks by protecting the keys with the hardware module.

In order to facilitate the use of the hardware module we need to look at the cryptographic key management and this is the part of the crypto requirement that are in the process of being updated. The idea is to have a permanent signing key for each voting machine that is linked to the voting machine serial number.

For each voting machine for each election, would generate an election signature and verification key and that would be used to digitally sign the electronic record for that specific election. After a specific election has been completed that signature key would then be destroyed after

that election.

So what do you get from this approach is you get digitally signed electronic records that prevent tampering once the election specific keys have been destroyed, you can't generated back dated records, electronic records. By having a permanent key associated with the voting equipment it helps to prevent substitution of machines or electronic records associated with that machine and it will facilitate the central tabulation machines, auditors and public in order to verify the digital signatures of those records.

Set up validation requirements. The goal of set up validation is to insure that the equipment is in the proper initial state. This is to address Resolution 6105, set up validation which is really focused on only authorized voting system software being installed on the system and no unauthorized software being installed on the system.

These requirements were based on VVSG 2005 requirements related to set up validation. What 2005 did really focused on the inspection of software installed on the system, checked to make sure that it hasn't been modified from a base line as well as the inspection of voting system register

and variable values.

What we've done is we've extended and modified those requirements. A lot of the modifications to the 2005 requirements relate to documentation requirements.

Some other new requirements that were created have to do with documenting a set up validation process for which the voting equipment was designed to support. So, that would be some user documentation that could be used by the user.

In addition, what we looked at was also expanded the scope of set up validation beyond just looking at the software installed on the system and the values of the registers and variables to look at requirement capabilities to support requirements. To inspect the remaining capacity of back up power supplies and cabling connectivity, is the communications active or non-active on the system?

Inspection of the level of consumables. How much paper is in the voting system? Inspection of the calibration of components that need calibration such as touch screens and things.

Inspections of external interfaces. How to inspect the external interface to determine that its in a secure state.

As well as to develop check lists of other voting equipment properties that the vendors would like to see checks when they set up the voting machines.

Finally, the creation of a record of the results of the inspections that are done. At that point –

MR. WILLIAMS: You've got a lot of things on this list that there's no way in the world a voting system test lab can test for.

A voting system test lab can't test for consumables in the precinct.

MR. HASTINGS: But what a test lab could do, is it could check for the capability to tell you the level of ink that's left in the printer. They could tell you the level – that's the type of thing I'm talking about. It's the capability to inspect things that are consumable. Paper in a paper printer. The printer I have at home has a spring loaded thing that as the paper gets less it goes up to zero.

That's what I'm talking about, the capability to inspect consumables used by that system, not at a given time of – so I hope that answers your question a little bit.

MR. SCHUTZER: Okay, so the intent of this is that you first of all know which machine sent which records because

of the cryptographic signing.

MR. HASTINGS: So this is back on the electronic –

MR. SCHUTZER: Jumping on that and then we will go back to the set up.

Assuming that's the purpose of that, and so when I go to add it up, if indeed if I had, you know independent software validation or something like that and I found a DRE suspect, I would be able to just eliminate those.

If I found one that was not suspect, I could count that. That sounds to me like a sensible thing to do.

For the set up and validation, I'm a little confused to in terms of am I testing the machines? I'm not sure how this works. If I go to a precinct, isn't the whole machine loaded with all the ink and the paper and everything set up or do I set some of that up myself or what is the point?

As the election proceeds I may have to do more ink. I don't know if that really counts but what I would like to see which I don't see here is some way of identifying who access those machines? Who is putting software in those machines? Maybe you have a two signature sign up for any modification or something such as that.

MR. HASTINGS: Those types of who has entered the

machine an that kind of thing that's actually going to be covered in the event logging, system event logging types of activities and requirements.

MR. BERGER: Nelson, I'm aware in some systems now, even the I-Pods, there's some of this technology being used to prevent any software that hasn't been authenticated by the right authority from being loaded, have you explored that concept here?

MR. HASTINGS: Actually this is something in software distribution and installation requirements that we are still working on. I know that I talked to you about this many weeks ago that it should be coming out. It just hasn't come out. We are exploring those types of technical concepts.

DR. JEFFREY: Any other comments or discussion? Okay. Well, deep breath Nelson.

I think when you look at the sum of all of the reports that we've gotten from the STS, Security and Transparency Subcommittee, we've got the preliminary reports that they have given us, covering eleven different TGDC resolutions from the past and with the additional guidance that was given in terms of the resolutions and some of the intents and one more potential resolution on the paperless, the subcommittee

views that the direction that they have outlined is the direction that they will continue to work.

Unless there is any disagreement, I would like to hear a motion to adopt the preliminary report that the directions that they have outlined are the directions for them to continue with the modifications that were made during the resolutions and discussion.

PROFESSOR RIVEST: Given the failure of the SI motion to pass, I don't know where we are left with that. We need to have some more discussion about that. Saying to continue on in the face of a NIST assertion that they don't know how to draft requirements for software dependent systems is something I don't comprehend. So I would seek guidance from the TGDC as to what we do in that area.

DR. JEFFREY: Okay, unless there is somebody who has immediate guidance, I think that is something that we may have to have people think about and be prepared to discuss later.

With that, I would like to then actually move to the next section and we will revisit this one. The next section is, who is up next? The Core Requirements and Testing Subcommittee Preliminary Reports. Is this Alan?

MR. GOLDFINE: Thank you Dr. Jeffrey. We've fallen behind schedule so I will try to move on.

I am the first part of an integrated CRT presentation, myself and David Flater are going to discuss a number of key issues. I think that's the live term within the CRT group - electrical, electromagnetic requirements, reliability, which in the context includes quality assurance, configuration management, accuracy and reliability benchmarks, metrics and test methods, COTS from a certain perspective, conformity assessment in the sense of VVSG testing, coding conventions and logic verification and some mention will be made, I think in passing rather than as a separate topic of the California volume reliability testing protocol.

We can then have a discussion at the end although the discussion at the end of the presentation may not occur until tomorrow.

Really, very briefly, I'm not even sure this qualifies as a key issue but it has come up in the past, our examination of the electrical and electromagnetic requirements within the product standard. This has been discussed in a couple of different directions. It was suggested, I think at the

last meeting, that we consult NIST experts outside of the voting team because there are outstanding NIST experts in electromagnetic and electrical requirements for electrical equipment.

We've talked to Boulder experts who are in the area of electromagnetic requirements, Gaithersburg experts for electrical requirements and codes and what have you. We have gotten some useful comments on the existing requirements and we will be shortly presenting to the CRT group outlines of possible revisions to what's currently there based upon these experts for discussion.

Just to mention this briefly, we are not presenting anything here in that area. This is just more of a status report.

The subject of reliability, a definite key issue. There are really two aspects when you talk about reliability with respect to voting systems. One aspect is how can we measure the reliability of a given voting system.

The other aspect, I'm not saying these aren't necessarily separate or even largely separate, but separating them the second would be what steps can be taken to ensure more reliable voting systems?

For the first area, measuring reliability what I'm going to do is very briefly give a very informal, very, very oversimplified outline of what is currently being done within the context of the current standard. I hope nobody jumps up and says, that's not exactly what we're doing. Its very oversimplified.

Basically we test the voting system, consider it is a self-contained black box, note the number of system failures during that testing, calculate according to appropriate statistical techniques, the likelihood that the voting system will fail during a period of time. This, in effect, gives us the mean time between failure metric and then if the results are acceptable, whatever that means, or whatever that is specific or interpreted, then the system passes the test. Roughly, roughly speaking that's what we are doing now.

This current approach in terms of both the method itself and the parameters has, as you know, drawn criticism for being insufficient. We have been discussing within the CRT group an approach that would integrate the testing for system reliability into the test method that's been proposed for system accuracy.

This has some advantages and disadvantages. Its somewhat a technical discussion. We are going to be discussing this in a few minutes. David Flater is going to be doing that as an integrated discussion of reliability and accuracy.

Why don't we leave any questions until that is actually been done. I just wanted to give you some background here as to why we are attempting to go in the direction that we are attempting to go in.

For the second question, the second aspect, insuring reliability, a research effort has been initiated. We have a research effort to investigate requirements for voting systems that would help assure maximum system reliability in a cost effective manner. There are two research papers that have been produced by your contract, Max S. Mayer (sic) that are out on the web. They have been there. You can read them. The first one basically has to do with reliability of voting systems in general. The second one more specifically has to do with quality assurance requirements and a possible approach to quality assurance.

The key idea coming out, emerging from this research, is the simple statement that you guarantee reliability, not

so much by testing a system for reliability, as by building it into the design of the system in the first place.

Some of the ideas emerging from the research some of which can be implemented right away, others perhaps are more longer term. Failures can be prevented through careful design and testing.

Voting systems should be designed in a modular fashion with well specified inputs and outputs. Systems should be capable, this is a more specific requirement, of using EML for data interchange. Perhaps not necessarily as the internal representation of the data but certainly for data interchange.

System software should be transparent, functionally verifiable and not contain code that is not used. That, of course, touches upon the whole COTS issue and, you know, really is an aspect of that.

Another specific proposal is that systems should contain a verification unit. A module of the system that can be designed to ensure that a given instance of the system about to be used is in fact identical to the one that was certified during laboratory testing.

Another aspect which gets a little bit into the

procedural area, but, you know, bears repeating is that ongoing gathering and analysis of the results from the field must be a mandatory part of voting system operations. We talked about this in the past that we need to ensure maximum feedback from the field, from the states, from the jurisdiction, to the Federal level so that we really know for sure what's going on out there.

Now, in one particular area an approach that we have been discussing would require voting system vendors to implement a quality assurance program that is conformant within the appropriate scope of operations to either ISO-9000-9001 standard. An investigation of this, or at least an investigation of the quality assurance part of VVSG was mandated by, I think its Resolution 30-05, a couple of years ago.

In the current VVSG, again going back saying this is the way its current done, then vendors can design and implement any program that ensures that the design, workmanship and performance programs are achieved in all delivered systems and components. Its also the case that the quality assurance program is the responsibility of the vendor who is required to provide test data and test reports

as part of the testing process.

However, the VVSG, the guidelines in the current VVSG might not be tight enough. This has been pointed out. It does not make use of any generally accepted standard that quality assurance programs would be required to comply with, relying instead upon a vendor developed program which, to some extent makes things inconsistent and to some extent requires vendors to reinvent the wheel and so on.

Also, essentially provides for the review of that vendor program, not early in the process, but at testing time, only after the quality assurance program has already run its course. That's a potential weakness.

ISO-9000-9001 is the recognized quality assurance standard. Its been successfully applied to product development in many industries. It is relevant and applicable to the development of voting systems. There's no reason to think that voting systems, at least I haven't heard of any reason why voting systems in particular, you know, would not be benefitted by ISO-9000 as opposed to other types of systems. It helps ensure that quality is built into the voting systems from the start and throughout development which is a key aspect throughout the entire

development process.

The ISO-9000 standard itself defines requirements in generic terms. This, however, as it well known, is not sufficient. Steve Berger pointed out possible horror stories that could be anticipated if simply hand waving for ISO-9000 were used where the vendor could say, yes, I'm fully conformant and this product meets my standard but it has an error rate of twenty percent or something like that.

Its completely true but as part of the process a quality manual needs to be developed that details the quality process for a vendor within the ISO-9000-9001framework. Even more specifically, this is where the VVSG must contain explicit requirements for the quality manual to ensure meaningful programs.

Sure, you could say that the generic ISO-9000 doesn't necessarily guarantee quality products, but that's where the requirements supplement it supporting ISO-9000 within a VVSG would come into play if, in fact, that's the direction that we go.

This is a diagram that we took from one of the contractor reports emphasizing the effect of ISO-9000 throughout the entire design, development, manufacturing, marketing and

post sales support life cycle. It has its effect all the way through.

If an ISO-9000 direction is agreed upon, we could require several choices. A formal certification through a third party audit, performed by a third party, in particular something accredited by the ANCI National Accreditation Board, which I think is standard for the third party audits for ISO-9000.

That should be rigorous enough for the EAC to rely upon. Vendor self-declaration of conformance, that's another possibility or even allowing the EAC to decide between A and B, in general or on a case by case basis.

So, I would think that one of the areas that we need guidance, whether its in the form of a formal resolution or simply a consensus, guidance from the TGDC is --. For quality assurance do we in fact head in an ISO-9000 direction or what do you say?

I've sort of put that general question out on the table and if we can either take questions now or immediately, you know, segue to David.

DR. JEFFREY: While you are up there let's see if there are any questions or discussion and if there is any comment

on the specific ISO-9000-9001 request.

MR. BERGER: First, I would like you to discuss in a little more detail what you see going into the quality manual or how you see that being developed.

MR. GOLDFINE: You, we haven't gotten to that point yet. We want to know, hey, is this the direction that we should take.

MR. BERGER: Well, just speaking for myself and this is Steve Berger. I apologize for not saying that at the beginning of the comment.

I think that's an extraordinarily important direction to go in. When you start writing quality manuals you are going to get deep into vendor processes and its going to be important that those be understood in detail so that they are harmonious.

MR. GOLDFINE: My idea, is probably not to write a process manual but to write requirements so that when the process manual is written, they will support the necessary goals of what we need for effective testing and certification.

MR. BERGER: I just would champion your statement. It think its extraordinarily important that we identify

what the characteristics and specific processes that we expect of all voting equipment vendors.

On the second part of your question, just my own opinion, is that ISO-9001 comes at a considerable cost. I think we need to see a cost benefit analysis as to whether that specific third party audit brings sufficient benefit for the cost.

MR. GOLDFINE: That's why I split that out as one of two or three possibilities. This particular point, in terms of well, is there a cost benefit analysis of this was brought up during the discussion surrounding Resolution 30-05 and it was pointed out at the time that NIST really wasn't the right organization to conduct such a cost benefit analysis. We should be providing technical recommendations and drafts and what have you and we weren't doing cost benefit analyses anywhere else within the standard.

Nothing to this effect was reflected in the wording of the Resolution, but, you know, the bottom line is no, we have not conducted a cost benefit analysis of this. What we are doing is giving you our best technical advice.

MR. SKALL: I agree cost is a question and it's a difficult one and we should try to get a handle on it but,

like Alan says, its difficult to do that. I'd like to just comment, I think the only alternative we really have in writing a standard is to say something like implementation shall conform to ISO-9000.

I think the question of certification, third party versus self declaration is for the EAC. Its not the type of requirement you would put in the standard itself. I think the question we have in front of us is, should we put in requirement for conformance.

That alone has cost implications but we really won't know the cost implications until we know how the certification is done and that's sort of outside our control. So its almost a Catch-22.

DR. JEFFREY: Thank you Mark. Any other questions?

MR. GANNON: In your presentation, you talked about how to ensure reliability and one of the points you made in there, I guess on slide 10, was about a system should be capable of using EML for data interchange. Earlier in the discussions we were having on software independence. I don't know that this point really got brought out as much and is there enough cross pollination going on between CRT requirements here and STS where transparency is a big issue

and use of an open format for exchange, not just export, is one way of achieving software independence.

Even what was looked at as future verification kind of systems where in fact, by having open interface, open data formats, you could have different vendor components in a system that also helps in the verification of various data formats whether it's the ballot record, whether it's the count, etc. So, what further information needs to be done to either evaluate that or to the point where the next iteration of the VVSG would use terms such as "shall" or "must" instead of "may."

MR. GOLDFINE: I think we do have to talk about it and coordinate that. The limited discussions we have had with STS, I think they are very supportive of the idea of using EML in that context. Excuse me, John wants to answer that one.

JOHN (?): We've actually talked about this for a good long time in STS and that there would be great benefit if ultimately all voting systems could produce records in a common format and EML seems to be one of the best choices. So, yes, we are very definitely considering that and we are working closely with CRT on that.

DR. JEFFREY: Ron.

PROFESSOR RIVEST: Alan I had a question about ISO-9000-9001. I have little familiarity with that and I was wondering if you could maybe educate me a little bit on what benefits there might be from a security viewpoint for using ISO-9000 process.

MR. GOLDFINE: Well, again, I think it, you know, a lot of it might have to do with the way the process manual is written. I can't think of any examples off the top of my head but if appropriate design and manufacturing techniques can be formulated that are appropriate within the planning of ISO-9000 that are security related, certainly they can be specified. In other words, the capability is there. I can't give you any specifics.

MR. BERGER: Alan let me just say I have been very encouraged by much of the work in reliability and the research papers you point out. I don't know that it came out as strongly as I think it deserves. Could you speak for a minute about the general movement I see on reliability to moving to probability of failure in an election type of metric as opposed to MTBF?

MR. GOLDFINE: Yes, we are getting right to that.

MR. BERGER: Okay.

MALE SPEAKER 27: I'll ask you one question on the ISO certification. Are there enough examples from other fields where you can show the, not a cost benefit, but just show the benefit of employing an ISO in terms of its end-to-end systems which might include things like security, reliability and other issues?

MR. GOLDFINE: Yeah, I think, there certainly are, I think we can certainly point those out. Certainly the auto industry and the aviation industry and what have you there are examples that can be shown. You think we should prepare a report or?

MALE SPEAKER 28: What specifically do you need the TGDC's guidance to be one way or the other today?

MR. GOLDFINE: Well, I think what we need is since we phrased it in a somewhat general fashion, you know, we are not saying specifically that the VVSG should require formal third party, you know absolutely require formal third party verification with all of the, perhaps all of the baggage that that entails. We are also – conformance to ISO-9000 that is –

MALE SPEAKER 28: Let me ask you in reverse. If this

committee said not to use that framework what would you do?

MR. GOLDFINE: What we do is, again, I don't know if you want to call it reinventing the wheel, but try to take the crucial requirements, the crucial procedures from the ISO-9000 approach and detail them, specify them as a series of requirements within the –

MALE SPEAKER 28: So what you are really trying to get away from is a vendor unique, vendor specified format in going to some sort of more overarching framework.

MR. GOLDFINE: Right and one that is defined, one that's recognized.

DR. JEFFREY: So, with that is there any comments or guidance from this group as to whether – is there any objection from this group about using that kind of framework?

Okay, I think you have got the intent of the committee.

MR. GOLDFINE: Thank you very much. David.

DR. JEFFREY: Since we started early and are running a little late, let's take about a fifteen minute break so that people can get up a little bit. So, be back by realistically, say 3:30, we are going to get started again.

(BREAK)

DR. JEFFREY: If I can again ask everyone to please

take their seats so that we can finish up the afternoon session or I will reopen the paper rolls discussion.

Okay, the next topic is continuing on the reliability and accuracy issue. David Flater will be the speaker. David, just drown them out.

MR. FLATER: All right. I can sort of hear myself. Okay, so I have a selection of presentations on a selection of topics and I thought that, depending on how the time goes, we could pick and choose which ones we actually want to hear.

I gather that we would like to hear about reliability first. So, I'm going to launch into that. Reliability and accuracy. This is a fairly long presentation so its divided into four parts.

First some background, followed by a discussion of a possible new reliability benchmark, new reliability test protocol, and then coming around and talking about how all this could be applied to accuracy.

So, first some background and in the background first a few terms that I'll be using throughout the presentation. First of all the word "benchmark" has a carefully written definition saying "quantative point of reference to which the measured performance of the system or device may be

compared." In plain language that means when we say benchmark we are talking about the number in the requirement such as 163 hours.

The word "metric" refers to a measure that we use to describe the performance of a system. For example, when we are talking about reliability, the metric that has been used so far has been meantime between failures which is time over the number of failures. When talking about accuracy we talk about a metric ballot position error rate which is the number of errors over the number of ballot positions. There is also a metric for ballot misfeed rate which is specified in VVSG applied in previous however there is not a test method specified for that as of yet.

Now, when we talk about reliability and accuracy the test methods for those have a couple of significant differences from the test methods that we use for other CRT requirements. First of all, it's the case that accuracy and reliability are general properties of the system, meaning they don't pertain to specific functions or specific things that you would do in a particular test case. You can collect data to evaluate reliability and accuracy during the execution of any test and the purpose of the test protocol

then is simply to tell us how to decide on acceptance and rejection of voting systems given that collected data.

The other significant difference has to do with what we are demonstrating using this test method. Most testing for core requirements can only demonstrate non-conformity.

This is what I mean by that. We have a specific function requirement saying that when the system sees A it shall do B. You can run a particular test case under certain conditions, give the system A and it does B. What that shows you is that under those particular conditions, the behaviors seem to be okay. It doesn't show you that in all cases the behavior is going to be okay. Whereas if you give the system A and it comes back with something other than B then you actually have an example to show that the system does not conform.

Now, the protocols for reliability and accuracy actually attempt to show to a statistical level of confidence that the system does conform, collects positive evidence to show conformity as opposed to simply trying to show that the system doesn't conform. In attempting to do this there are compromises that I'll be going into in future slides.

Now with respect to the big picture on these benchmarks, first of all there is a big conflict that we need to acknowledge which is that in most cases conformity to strict benchmarks cannot practically be demonstrated through operational testing. It just takes too much testing to collection sufficient evidence to give positive evidence of conformity to one of these benchmarks. It's a strict benchmark.

On the other hand if we set a relaxed benchmark it simply doesn't accomplish the goal for which the benchmark was set. If you set a lax benchmark, then even a bad system is going to satisfy the benchmark. So, it becomes difficult to reject bad systems.

In other industries this conflict has been addressed using available methods for design, quality assurance and performance monitoring by which I mean reliability is built into the system from the very beginning. It is a very rigorous process to build reliability into the system. Alan talked about this a little bit and there is research reports that talk about this in some detail.

This presentation is more about the little picture which is simply what do we do about evaluating reliability and

accuracy within the VVSG itself. Compromises have been made in order to accomplish this goal of demonstrating conformity. Its been compromise from both directions both in terms of the testing itself and in terms of the setting of the benchmark.

With respect to the testing, VVSG 05 permits test labs to bypass portions of the system that would be exercised during an actual election. There is a bunch of language on this slide and like all standard language its subject to interpretation.

The bottom line is for DRE systems where you have a ten finger interface to the system. Sometimes a complete system test is done for reliability and accuracy up to a certain point, up to the limits of our ability to actually generate input to the system in a pragmatic fashion, but for the most part, these systems are run using a simulation, an internal simulation that bypasses the ten finger interface.

Although the language of the spec here says that in the event that only partial simulation is achieved then you will validate the proper operations of the other parts of the system. It is not the case that testing component A

and testing component B tests the system. Unless you test the entire system together, you really have not conducted a valid system test.

The benchmarks have been something that have been discussed quite a bit in terms of the ramifications thereof. The V requirement that appears in the product standard says, "the mean time between failure demonstrated during certification testing shall be at least 163 hours".

A lot has been said about the 163 hours and that this is, according to most reviewers wholly inadequate. As it happens, the benchmark that is demonstrated in the testing is not that. The mean time between failure that is demonstrated by the testing that is specified in the standard, ranges between 44 hours and 73 hours at 90% confidence.

The minimum duration of the test using the protocol that is specified in the standard to demonstrate that is 169 hours. That was increased from 163 hours as of 2005 as a result of a new calculation of the numbers that were in there. Essentially the numbers that were in 2002 and 1990 our statistician could not reproduce them. Using an old handbook, 791A, I think it is, the numbers were regenerated and they came out to be 169 hours instead.

The bottom line is that there appears to have been some confusion with regard to the 163 hour figure as it is cited in the original requirement. In fact there is some discussion surrounding the requirement in the product standard that discussed a 45 hour scenario in which for a given election there will be 30 hours of set up followed by 15 hours of actual during election day use. So, there was sort of this discussion given to justify a 45 hour figure but then the 163 hours is what actually appeared in the requirement. So, take from that what you will.

The chart on slide 12 shows some of the ramifications of the three different benchmarks that appear in the current standard. The 45 and 135 hour benchmarks are the lower and upper test meantime between failures to use the parameters to the test method and I won't go into detail explaining the difference between them. Whereas the 163 hours is what actually appears in the requirements.

For all of these if we look at what the probability of failure would be, given a system that satisfies these benchmarks, probability of failure in 15 hours for a 45 hour benchmark is 28%. In other words, you can expect 28% of your voting devices to fail by the end of election day.

The best of all benchmarks appearing in the current spec, the 163 hours gives you a probability of failure of 8.8% in 15 hours. So, you have a question?

MR. SCHUTZER: What we are testing is actual equipment or is it just we have specified? Is this what we really expect in the field?

MR. FLATER: The benchmarks are taken from the spec. The probability of failure is based on the statistical model that is used.

MR. SCHUTZER: No, no, I understand that, but I mean the numbers. Are these derived from just what's on the spec or is this derived from what – have we actually tested equipment and come up with these numbers as being realistic?

MR. FLATER: These are from the spec.

MR. SCHUTZER: So, it would be interesting to know what's realistic in today's equipment as to whether one would experience this kind of failure rate. Its fairly high.

MR. FLATER: We have heard various anecdotes but those are not facts that I would enter into the record at this point.

MR. WAGNER: I can give one data point on this which highlights that things are maybe could have been even worse

than David Flater brought out.

When California conducted its first volume test they were able to get a pretty good measure of the reliability of the system in circumstances that probably would be representative of real election. It was an actual test of the full system without this simulation bypassing the user interface. My rough estimate from the data that we got of the reliability of those machines which had been approved by the testing labs was about 15 hour, one five hours NTBF (sic). So that works out to a probability failure during one day of election operation of pretty high, over 50%.

Now that machine is not in use, those problems were fixed. Those flaws are not present as fielded today but I think that indicates the impact of the failures in the methodology that particularly impact bypassing part of the system. In that particular case there was some problems with a part of the system that had been bypassed and consequently were not tested by the ITA.

MR. SCHUTZER: So you are saying that inexperience when you ran the equipment they experienced even worse than these numbers. Now when we have failures like that are we talking about failures which are like hardware failures where that

box is then out of commission for the rest of the day or are we talking about something which could have been re-booted, for example, and started up again?

MR. WAGNER: This is only one data point and since then there is some reasonably, this is not typical of most machines. In that one case the kinds of failure we are talking about were paper jams and freezes of the machine, crashes essentially. Whether those could be recovered from depend on your procedures. If your procedures said, if it crashes unexpectedly, go ahead and reboot and continue using it, you could continue using it.

On the other hand its not clear whether those are procedures which we should be very comfortable with because at that point the machine is in an unknown state.

MR. SCHUTZER: One last question is that, when you reach these things like paper jams, I can understand how to deal with that. The freezes the concern there would be has the system been designed so in light of those failures the votes are not lost?

MR. WAGNER: It should be.

MR. BERGER: One clarifying question. Your percent of failures column, is that assuming a galcean (sic)

distribution of the failures?

MR. FLATER: Exponential.

MR. BERGER: Exponential distribution. So I assume that I would be right that if the failure mechanism were something other than say, perhaps, produced a rectangular distribution, these numbers could look very different.

MR. FLATER: Yes.

MR. BERGER: In other words, you could see no failures and then you hit where the rectangle starts and you see this tremendous percent of failure across some threshold.

MR. FLATER: The distribution that used as one that is appropriate assuming that the burn in period for this equipment is over. There is a set of assumptions that goes along with it. So, yeah, of course, depending on the model that you choose, you would get different numbers.

MR. SCHUTZER: So it sounded to me, I mean just jumping to something here, there is two types of problems you are facing. One is the paper problem and we have discussed also ad nauseam, this morning and ways around that.

The other is the standard problem in software, particularly off the shelf kind of software that often times

freezes. The appropriate number to look at then is really availability as opposed to mean time between failure and the ability not to lose any data.

In other words that is to say its not the end of the world if a box fails in 15 hours, particularly if you have the right kind of procedures in how to get it back up and running again in a fairly short order of time. So, the availability was like 98 or 99 percent, it only was a one minute downtime. As long as they didn't lose any votes.

So, I'm wondering if – first of all its bad to not test it with volume. I know we addressed that. Its bad not to test to the actual experiences. We had to cut out different parts of the components but also one should really be looking at availability in that mean time between failure.

MR. FLATER: We've gotten conflicting advice on availability. The advice that we received during the review cycle for VVSG 05 essentially said this is not useful to include in the standard because this analysis is on the assumption that you would be repairing equipment and putting it back into service on election day.

The feedback we get says that if you actually do this, as an election is in progress, you have problems with how

do you prove to people that this wasn't an act of tampering.

With respect to the reboot case, there are a lot of questions about what the effect on the integrity of the process is going to be if we are going to make the assumption that okay, every X voters we are going to have a spontaneous reboot of the system.

There are different ways to address the reliability problem. You can treat voting systems as consumables. They burn out in one day and then you replace them. If you want, you can do that. Being responsive to the feedback that we have received so far, what we've heard is that we would like higher reliability.

MR. SCHUTZER: Well, we would like higher reliability too. If you are going to specific reliability that turns out to be impractical for the class of devices (not speaking into mike). Of course there's swapping and having spare printers if the jam is one thing. Having a few spare computers if there is hard failures is one thing but if its not a hard failure then you have to face the facts that, (not speaking into mike).

Many of the devices we use in banking when they do go down and they do get restarted doesn't necessarily mean there

was any loss of data or any loss of availability. I mean you have to take that into consideration. If you are going to put in reliability numbers, you should have reliability when you put in numbers that would be not (undecipherable) in today's state of the art considering the total system. Are you going to put in reliability plus availability figures and have yet to get into the procedures and into the kinds of testing (not speaking into mike).

MR. FLATER: Steve, did you have something to say?

MR. BERGER: There was something I wanted to highlight in what Dan just said. It struck me as quite important and that was the point of failure mode. The reason it caught me as important was potentially we could be more relaxed on some levels of environmental stress if we knew when a piece of equipment failed it was going to fail safe if you will. Do we, in the standards, identify that kind of concept?

MR. FLATER: There are general requirements to the effect that no matter what happens, the votes shall be recoverable.

MALE SPEAKER 29: (Not speaking into mike).

MR. FLATER: I think that would assume a small and

finite set of faults. Essentially that translates into a negative. The system shall not lose votes under any conditions. So, that's an infinite field of test cases.

MR. BERGER: Well, if I may going back onto the paper jam issue. If the system could detect successful printing and record almost like a provisional vote, those votes that weren't successfully printed so that they can then be printed out later, that may help with some of those issues.

MR. SCHUTZER: And shall not be both – well, lets put it this way. In the transaction processes system, what we'll say is it shall not lose any transaction that has been completed even if the system fails. If the system fails in the middle of a transaction, that vote, that transaction will have to be re-entered.

MR. FLATER: The transactional model makes a lot of sense for a voting session, I think. The only place we have run into trouble with that is, I believe, in the case of fleeing voters because we have local law saying, in some cases, you can't roll back that transaction even though the voter has not completed it and gone to the cast vote.

There is local law saying essentially someone is going to step in and commit that transaction. I suppose from the

equipment point of view, you can simply by agnostic about that, but in terms of how we define the transaction, it's a little dicey.

MR. WILLIAMS: Transaction on a voting machine is when you hit the cast ballot button and the way all of the current machines are designed you would have to have an almost instantaneous failure at the time somebody did that for that device not to record that vote.

The fleeing voter thing, there is two schools of thought on that. One school of thought is that if you leave the voting machine in a suspended state, you just cancel the vote because otherwise I would be voting for you. If you want to talk about fraud I could certainly go through your ballot and change anything in there I wanted to.

The other is that whatever is in that machine is the intent of the voter and you should cast it and I know of states that have both of those laws. Some cast the ballot for the voter that fled. Some cancel the ballot.

On the matter of transaction to me that's pretty clear. The way the current machines are designed, it would be a pretty unusual circumstance where you actually lost a transaction.

MS. QUESENBERY: This is Whitney. David, you've laid out a rather interesting conundrum because we are constantly talking about how hard is it to achieve the result we want. Do you actually have an answer?

MR. FLATER: There is quite a lot more to this presentation.

MS. QUESENBERY: I wonder if we could move on and hear what you think the answer is because I think its really clear what the conundrum is.

MR. FLATER: Okay. Where I was, I was talking about the benchmarks currently in the spec. Given these benchmarks, what's presently done, the 169 hours of testing provides 90% statistical confidence that the true meantime between failure of the system is at least 45 hours. That takes a week of run time. If we wanted to demonstrate the same level of confidence using the same test protocol for what the requirement actually says, which is 163 hours, it would take 25 ½ days of run time or four devices if you want to complete in the same amount of time.

We have received some advice regarding what the meantime between failure benchmark should be. The lowest of the advice we have received was that it should be 1500 hours which would

give a 1% probability of failure during a 15 hour election day.

Using the same test protocol, same parameters, etc. if we want to give 90% confidence that the system conforms to that, to demonstrate that, we are looking at 234 days of test time which means, if you want to get it over with in a week, you need 34 devices running parallel or, if you happen to have 100 devices as in the California reliability testing protocol for DREs, you have to rack up 2.34 days of run time. This is already 9 times as long as the California volume test as specified.

Now, the 1500 hour benchmark was in fact on an early IEEE draft and the number was later increased to 15,000. In the public comments on VVSG 05 the range that was proposed to us was 5,000 to 15,000 hours and the test times to demonstrate these benchmarks is correspondingly worse.

We are in the realm where its quite realistic to ask the question whether practically we can rack up this much run time with real voting systems. That's an understatement, I think.

There are certain kind of devices and certain kind of situations where its very easy to rack up a lot of run time.

They are completely non-interactive devices and voting systems aren't.

So, as a data point to tell us what level of testing, how long a testing could actually be tolerable, I give you the California volume reliability testing protocol for DREs because its actually been done. We know for a fact that this is feasible. This test uses 100 devices, 50 people acting in the role of voters over a 6 hour time span, casting 110 ballots on each of the 100 DREs. The protocol specifies acceptance if up to 3% meaning up to 3 of the machines suffer what are defined as substantive failures. This is actually the lesser category of failures that's defined in the protocol.

The good news about this test protocol is that it is a real, valid system test that uses real people interacting with the equipment in the way its intended to be used and in practice, it has given results that were useful to the State of California that were not uncovered in the Federal certification process.

The bad news if we go back to the analysis of well, what performance is actually been demonstrated is that if we run up 600 hours of run time with 3 failures and we want

90% confidence in the result, we have only demonstrated a mean time between failure of 89.8 hours which still gives the 15% probability of failure in a 15 hour election day. If we had zero failures we would demonstrate 260.6 hours which gives a 5.6% probability of failure during a 15 hour election day.

However the distance between what has been demonstrated here and what was proposed to us to demonstrate in public comments is still quite vast. So what can we do about this? We can in fact improve the impact of testing without making it impossibly by making some changes within the framework of the standard we now have.

First of all we use a realistic volume test. We don't simulate the volume. We do it similar to the California volume reliability testing protocol.

We eliminate the lax benchmarks which cause us to tolerate many failure that occur during the testing. We make full use of data collected throughout the entire testing campaign instead of designating a particular closed test regarding accuracy and reliability.

However we must acknowledge that quality cannot be tested in, it must be built in. Our ability to demonstrate

reliability and accuracy during a test campaign of reasonable length is quite limited. So, if the goal is to have a really, really reliable voting system it's going to require changes in the entire process.

We will now go into discussion of a new reliability benchmark. You raised the question what kind of benchmark do we want? Meantime between failure has been in there since 1990 however if we think about it meantime between failure says nothing about the workload that the system is under. It just says you run it for this long and expect this number of failures.

Realistically voting equipment is unlikely to fail (undecipherable). So, given what we know about voting systems, just a high level of common sense analysis would seem to indicate that in volume dependent benchmark would be preferable because certain categories of voting system failures are arguably related to the volume and less so to the time.

Now volume means different things to different sorts of voting devices. A great many of them, we can characterize volume in terms of the number of ballots or the number of ballot positions or the number of votes or concepts

comparable to those. However if we look at something like a central election management system that's just being used to get totals from precincts and generate high level reports, etc. or any MS that's just being used to do ballot styles, those concepts of volume really aren't relevant to that equipment. I'm not sure exactly what the bottom half of the metric should be in the case of that equipment and I'm expecting to get feedback on that at some point.

For something like a smart card activator, number of ballots, number of ballot positions of votes isn't relevant but the number of voters is relevant which is the same as saying, close to saying the number of smart cards. Smart cards is what you would use to actually test.

The good news is given these differences in equipment we can specify different benchmarks for different types of devices according to whatever concept of volume or time is most appropriate to them. To the test method itself, a ratio is a ratio. For collecting this data or crunching some numbers, whether those numbers refer to the number of ballots or the number of votes, what have you, really doesn't matter from the test method point of view.

The question is probably on the forefront of many

people's minds is what should the new number be if not 163 hours? This depends on the sort of feedback that we would get in terms of what proportion of voting devices election officials are prepared to have built during an election.

If I can be provided with that number as well as the way that those election officials measure volume for those devices over the course of an election, if you want to continuing using time we can do that. We can specify volume in terms of the number of ballots or ballot positions or whatever and also any assumptions that you have that would also affect the way the system performs. Given these numbers we can calculate a benchmark.

If you only want one benchmark then we need to choose this proportion of devices that fail as well as a measurement of volume to be applicable for all devices. That doesn't necessarily have to be so. You can specify one kind of benchmark for both capture devices and another kind of benchmark for central account tabulators. I think that would be very appropriate.

Now, I will move on to a discussion of a new reliability test protocol. The current test protocol –

DR. JEFFREY: May I just ask a question? The last

one in terms of the numbers. Do we have access to data from the most recent election as to actual failure rate, the number of failures in different jurisdictions and therefore could be tied to different classes of machines?

MR. FLATER: I don't have it.

DR. JEFFREY: Is that something – Commissioner Davidson is that something that's normally collected? It would be literally the number of failures in different jurisdictions. If yes, then, excuse the bad phrase, the benchmark is to what we current have actually.

COMMISSIONER DAVIDSON: Currently we do not have any data on that. That will be part of our certification program in the future starting in January. So, right now we don't have anything to help you on it.

DR. JEFFREY: Thank you.

MR. FLATER: Moving on to the test protocol. Issues with the test protocol as currently specified. Firstly, as we have discussed, is it allows the use of simulated volume which compromises the value of the test. Also, it has a high tolerance for failures that are observed during the test. This, of course, relates to the benchmark that's specified but also to the test protocol that's used.

The bottom line currently is that up to 6 failures are tolerated just during the testing campaign. Of course, you cannot expect the performance of the equipment after its fielded to be better than what you saw during testing.

A more tricky problem is the assumption of the self-contained test. If you look at the current standard it seems to say very clearly that the testing for, the evaluation of reliability and accuracy are done concurrent with and exclusively within the testing, the environmental testing for temperature and power variation tests. Something like that.

This was convenient at the time because this test runs for a certain amount of time that is commensurate with the test protocol for reliability but this leaves us in a bind if, supposing the equipment does fine during that particular phase of testing but then we start seeing failures in other parts of the test campaign. Presently, as far as I can tell, there is no protocol in the standard telling the test lab how to consider failures that occur elsewhere in the test campaign.

The evidence that I have seen, as far as I can tell, we look at failures that occur during that particular test

and when they occur elsewhere, they are sorted of handled (undecipherable) this is an operational failure that we have to deal with but it doesn't get factored into the benchmark as far as I can tell. That's cause for concern.

Finally, if we stick with the same test protocol, the duration of the testing meaning how long we have to test, is forced on us by the benchmark we choose and the test parameters that we choose.

So some possible changes to the test protocol firstly, it is perfectly feasible to collect data across all valid system tests that are conducted during a test campaign. There will be a few exceptions. Strangely enough right now, the test that's specified is specified to occur during an environmental testing when the unit is in the test chamber being alternately heated and cooled and subjected to other tortures.

If we want to run a complete system test using real user input, this is probably the last place that we want to require data collection for reliability and accuracy. Its an odd situation.

We could collect data across all tests except those that would require us to put people under harsh conditions

and require that one of these tests be a good volume test similar to the California volume reliability testing protocol. We can reject the system if after observing a failure, the data collected show with 90% confidence, that the system does not conform even on a single failure. Common sense says if you set a high benchmark for reliability and you witness a failure during a test campaign of a very short length, the chances statistically speaking, that the system conforms to that strict benchmark are less than 10%.

At the conclusion of a successful test campaign we can report the system performance that was demonstrated with 90% confidence. This will vary depending on what exactly we observed during a test campaign.

It varies current as I said between 44 and 70 some hours. If we are going to set a very high reliability benchmark or even a moderately high reliability benchmark, it would be unrealistic to require exhaustive testing to demonstrate, in a positive fashion, conformity to that benchmark with 90% confidence because we get into the situation of requiring very, very long testing.

So, it’s a trade off. Something has to give if we set a strict benchmark and we require positive demonstration

and 90% confidence, we get into this very long testing scenario. If we set a lax benchmark, even bad systems can get certified. If we want to keep the strict benchmark, then we can't require exhaustive testing.

MS. QUESENBERY: I just have a question. An accessible voting system is really multiple systems in one because its not only the visual touch interface, for example, but it might also be an audio tactile interface, is that two separate tests or is that a single test? How do we handle that?

MR. FLATER: Speaking off the top of my head, I believe that these extra interfaces which attach to a DRE presumably, these would all be considered components of a DRE. Over the course of the test campaign, you would test these various different interfaces so the reliability observed of these components would have an impact on the reliability observed of the DRE.

MS. QUESENBERY: One other off the top of my head question. I was very intrigued by the California volume test which I think I understand. One of the objections to usability testing has always been how are you going to get that many people in one place…

(**END OF AUDIOTAPE 3**)

* * * * *

(**START OF AUDIOTAPE 4**)

…different part of the test area to be part of the usability test or to even combine those. I mean is that worth investigating?

MR. FLATER: I would do it in the opposite order because –

MS. QUESENBERY: Obviously, yes, you would want to do it in the opposite order, but is that something worth considering and pursuing?

MR. FLATER: Clearly we have, in terms of testing CRT requirements versus testing HFP requirements, we end up with the same sort of demands, if you will, of what sort of testing needs to be done with regard to these requirements. I do believe that some synergy could be constructed here as you said, we could treat the learning process. When the people are coming in untrained this proportion of the ramping up process for them would be a good usability test.

To the extent that they are making mistakes during the learning process, these would not be good input to the assessment of system reliability. So, you almost want to

transition.

MS. QUESENBERY: Right, so you might end up with just a synergy of test set up and personnel involved, but not necessarily a synergy of results.

MR. FLATER: Yes.

MS. QUESENBERY: And the other point I'd just like to throw on the table is that when we think about who those 100 people who come in the door to test, it would be nice to make sure that they were appropriately selected if. For the reliability test it probably doesn't matter although if the point of having a real human is to generate diversity of human behavior in dealing with machines then you would want to make sure that people of different ages, different language abilities, different physical abilities were all included.

MR. FLATER: Certainly and I think, I do believe –

MS. QUESENBERY: You know, they just up the requirements, but –

MR. FLATER: I agree that what we are looking at here for practical purposes is one big test and not two big tests.

MR. BERGER: David, you asked for feedback on the self-contained test issue and if it would be helpful to you

I would be happy to make a resolution, but I do believe best value would be for the test lab to record any failures, no matter where they happen in the test campaign. If they start to see a pattern, then that's a cause for investigation as to what the underlying causes are.

I've see that where sometimes into one stress there is a latent defect that doesn't show up for sometime. This kind of thing can be helpful in identifying that sort of thing and sometimes having to craft the test case.

Does that mirror your thinking on this point?

MR. FLATER: Yes. You never know when the failure is going to happen and I just think that it doesn't make a lot of sense to have a test protocol that doesn't give you a way forward when failures are observed in other parts of the test campaign.

MR. BERGER: Would it be helpful to have a resolution on that?

MR. FLATER: I actually didn't think that was going to be an issue of contention.

MR. BERGER: Let me suggest what we do because thinking down the road to a vendor with a test lab engineer who is not in this process. That would be a point that could

easily be challenged as the appropriateness of becoming alert to a pattern of failures that happened outside of specific tests. I think certainly my opinion would be if there is an observed pattern of failure anywhere in the test campaign, that's certainly appropriate for that to be explored and potentially fail a system.

MR. FLATER: Okay.

MR. BERGER: I'll just make a motion that requirements be put in that tests not be written as self-contained, but failures observed during the test campaign those can be explored as to their cause.

DR. JEFFREY: If I could suggest that perhaps we introduce any additional resolutions tomorrow because I am conscious of the time and the 62 additional view graphs. That way we don't do the committee writing of the proposals like we did before. If you could perhaps draft that tonight and introduce it tomorrow that would be great. Thank you.

MALE SPEAKER 30: You asked for feedback on the reliability. First I wanted to say I think you and the CRT team are doing a great job. This is really outstanding and will be fantastic.

You asked about the trade off between the benchmark

and the testing methodology and my take on that is I think we would be best serving our voters by focusing on proving the test methodology as our first priority and making only modest improvements on the benchmark, on the number.

My other comment that I want to throw out there for consideration is, we may want to take into account that the impact of failures may be different in different voting classes. For instance, if a failure occurs and an op-scan machine is rendered unusable, voters can continue voting and the ballots can still be accepted. The impact of that, while you don't want to have those failures happen, its not absolutely devastating.

For instance, on a DRE if the machine fails then the machine is unusable, now all of a sudden voters can't vote on that machine and the impact may be more severe. I don't know whether anyone has considered different standards for different classes of machines, maybe that's not a can of worms we want to open.

MR. FLATER: Maybe I should go back a couple of more slides. We can specify different benchmarks for different types of devices. In fact, in the current standard although there was one reliability benchmark, its actually

interpreted into different benchmarks to the expedience of specifying a different volume for precinct count than for central account.

MR. SCHUTZER: A more general way to do that is not so much –

MR. FLATER: Your mike's off.

MR. SCHUTZER: -- not so much by the type of device but at the point in the voting process by which the failure would be felt the impact of. So, are you simply saying in the optical scan devices, a failure of the optical scan device doesn't really impact you in the actual voting process, its in the tabulation later on. IF you had a more general way that would be important.

I think also its important to talk about the nature of the failure. One that's recoverable versus one that's not recoverable. I think if we continue on this way in terms of really defining what our numbers are, what our test procedure is and what kind of failures we are talking about and what points in the various parts of the voting process, that will get us to where we want to be in terms of the mean time between failure and the availability and all those kinds of numbers.

MR. FLATER: No more comments? All right, I didn't do this yet.

So, finally I'm coming around to accuracy. The benchmark for accuracy is specified as a ballot position error rate and the benchmark that is in the spec now, I do not think could be described as a lax benchmark. The lower test benchmark is one in half a million ballot positions is allowed to have an error. There is a target benchmark of one in ten million, but, once again, we what we are actually demonstrating to 90 percent confidence is the one in half a million.

The issues here aren't with the benchmark so much as with the way the metric is defined. We still have the issue with the simulated volume, with the validity of the system test. We want to make the same changes here. The metric that's in the standard is ambiguous in terms of confusing ballot positions with the votes.

I research this going back to the 1990 standard and in 1990 it talks more about votes and less about ballot position, but the confusion seems to have been building all along. As it is its unclear how inaccuracies in anything other than the vote total for a specific candidates is going

to be included in the assessment of accuracy. For example, if we have a report of the number of ballots in a particular precinct and the totals of under votes and over votes, if all the tallies for separate candidates are correct, the protocol doesn't really give us any input on how do we count errors that appear in these other reported totals.

MR. SCHUTZER: If I may, based upon the feedback I'm getting from the test results, the problem here is the real issue and accuracy is not so much in the accuracy of the machines or the accuracy of the software, but the accuracy of the human interface to the machine. That is to say, if its optical scan its how humans really do mark the ballots.

If it's a DRE, how humans really do touch the touch screen and the kinds of inaccuracies that you get there seem to be overwhelmingly greater than the inaccuracies with testing in the software or the hardware components of themselves.

MR. FLATER: I won't argue that point however, there are issues with the test method for accuracy.

I don't think there is any argument with the point you made. Certainly, what is the biggest enemy of getting credible election result totals just in terms of counting

votes. The biggest enemy is getting the intent out of the voter. Once the intent is out of the voter, once we have some quantity – I'm sorry, that's a strange way of putting it.

MR. SCHUTZER: I didn't mean the fact that the voter gets confused and votes for the wrong person based upon the design of the ballot. I meant just the nature of the, I know its going to be harder to test for accuracy, but its just the nature of the way in which the voter actually interacts with the device in terms of their finger touching something and maybe not recording it correctly or their pen not fully filling out a circle enough or dark enough to have it counted properly.

I think something would have to be included in the testing somehow, even though I do agree it makes it much more a manually intensive type of a test.

MR. FLATER: Voting can be viewed as a kind of measurement and what you are trying to measure is voter intent. You are starting from this abstract and you are trying to boil it down to a number and most of our concerns about the performance of this measurement are being handled in HFP through the usability whereas what we are looking at in CRT

here is simply the benchmark and the test method for accuracy. Once we have gotten beyond that point, once we actually have the numbers in the equipment and we want an evaluation that the equipment is going to do the tallies correctly from that point on.

MR. SCHUTZER: I guess the appropriate thing is that I will have to wait for that report but that is not being specified and investigated (mike was off and I could not hear what he was saying).

MR. FLATER: I'd say they are on it. I'd say they are all over it.

DR. JEFFREY: We will get the briefings tomorrow morning on that.

MR. FLATER: So back on the issues with the accuracy testing as it stands, I discussed the issues with actually the metric that's used to count the errors that appear in a vote data report.

There is also an issue with the way that the benchmark is specified in terms of low level operations which are not easily testable. The changes that have been discussed have been to use a single end-to-end accuracy benchmark for testing purposes.

It certainly makes sense to have benchmarks on the accuracy of low level operations as design guidance and we are talking about things like detecting marks off of the paper as one operation, putting these into flash memory storage and other operations. We would like each of these operations to be trustable but these are not, these are invisible if you are just looking at the system level. What we see are votes go in and a report comes out. These are the observables. These low level benchmarks make sense as design guidance but for a tester it would be must simpler to have one end-to-end benchmark for testing.

With regard to the ambiguities in the metric, I'm going to discuss on the next slide the idea of report total error rate as a replacement for ballot position error rate. Finally, for the testing protocol itself, we can use the same protocol that I discussed with regard to reliability in the assessment of accuracy.

We have to harmonize the model. In fact this turns out to make a negligible amount of difference in the actual numbers you get. We harmonize the level of confidence that we want before me make a decision to reject the system.

About this metric for report total error rate, what

is needed is a definition of error that allows them to be counted. Give something observable such as a vote data report after running a test scenario, tell me how many errors were made.

It is just one error? Is the report just right or wrong? Is the tally being off by one as bad as being off a million or is being off by a million no worse than being off by one? How exactly are we going to assess errors here? Its not as simple as the current guidelines imply. There would be zero or one errors for each ballot position. There is an abundance of possibility for error throughout the system. We don't necessarily map one to one with ballot positions.

Next slide shows language for the actual definition. I won't go into details on this except to apologize for the stilted language. This is an attempt at making a more precise metric that nevertheless will solve all the problems. We can work on the language, I guess.

This is the last slide in the accuracy and reliability presentation. Something that is still to be dealt with is the granularity of the benchmarks. Currently it looks like reliability should be specified at the device level while

accuracy should be specified at the system level.

The reasoning is this. Reliability of the system as a whole depends on how many devices you have in the system. The more devices you have the higher the overall failure rate for the whole system would be. It seems to be the case that when we assess reliability what we care about is reliability at the device level.

Accuracy on the other hand is a system level concern. We want to know when we get reports at different levels whether these are accurate. We don't care so much about how many devices went into the determination of that report. This report is a summary of an entire jurisdiction and we still want it to be quite accurate.

Input is needed from election officials to help determine what the specific benchmark should be. (Undecipherable) an acceptable percentage of failures, the reasonable range would seem to be between zero percent and thirty percent based on – if you look at the lowest benchmark we have so far the 45 hours, that's 28%. So, that seems to be the reasonable range.

Also, an acceptable number of errors in the election. If we interpret error in terms of report total error rate

which talks about just how far off the tallies are, its not one error assessed for an entire long report. Applying the current benchmarks to a state the size California results in an acceptable number of errors – less than 1,000. So, I think the reasonable range for that is probably zero to one thousand.

Also specify the volume or time if you prefer for each type of device and from this we can work to a testable benchmark. Yes,

MR. SCHUTZER: I buy a little bit of what you say about reliability at device level versus the accuracy at the system level. Two points.

One is if we don't forget the fact that availability enters into the equation, availability is tied into the procedures by which people operate and maintain the systems and how they go about getting it back up and running, how many spares they have and so forth, that aspect of availability should be at the system level the same as the accuracy.

A suggestion I have is that it would seem to me that one comprehensive test could be done which could drive both accuracy and availability figures at the same time you don't

have to run multiple tests. You could even accomplish that if, depending upon how well coordinated the human factors, those aspects of the accuracy as well.

MR. FLATER: We can generate volume, understanding that we are going to assess these availability and reliability throughout the test campaign we certainly want to have a good volume test. We can generate volume in a volume test that will be used in the assessment of both reliability and accuracy. Whether its at the device or the system level, we are still collecting data during the same test.

MR. SCHUTZER: I agree that reliability at the device level but one might consider thinking about one which might be very useful to the field is what kind of test could you derive which could, out of that test, provide both availability measures and accuracy measures and take into account the accuracy not just of the software and hardware but the human accuracy aspect of it to. It will give you one test could provide those three streams of numbers for which one had benchmark numbers, one would have derived for you what’s acceptable or not acceptable.

MR. FLATER: The tricky thing about evaluating

availability through testing is that you need failures. Failures are something we hope we don't have.

MR. SCHUTZER: From what we've seen (mike is off, cannot understand what he is saying).

MS. QUESENBERY: I'm not convinced that you can get – the whole point of the usability test that we are working towards is to be able to have a benchmark for minimum error rates, but I'm not sure that this same test will give you both the volume for reliability and accuracy and also human performance errors.

As we have talked it could be combined up into one big day where there is sort of two tests going on simultaneously but –

MR. SCHUTZER: Well, it seems to me that if you had a simulated environment and tried to parallel the experience in terms of the volume and people coming in and trying to perform certain tasks and you ran it for a duration of time, you are going to pick up, and you also had in the middle of that also the practice of the procedures and how you get things back up and running. At the end of the two or three days worth of testing, you would have a good measure of the human errors, in terms of fingers not touching and things

not being marked and stuff like that, you would have a good measure of the availability of the equipment.

MR. FLATER: I'll agree with Dan to this extent which is if we are running this grand unified test and we observe an anomaly and its been explained to me what this term means, this means something that we think is odd but is not necessarily been attributed to a system defect or user error or anything in particular yet. We track the anomalies. Those that are attributed to "human error" deserve further investigation as indications of a possible usability problem with the system. Those that are attributed to equipment failure, machine error whatever its called, these then deserve further investigation from the reliability, accuracy, etc. point of view.

There is this test design issue in terms of getting a well designed, usability test and not having interference between that and the test design for reliability, etc.

MS. QUESENBERY: I think that there's no question that in usability tests we turn up quality problems and vice versa. So, to be able to have cross talk on the results and be able to use the results in both cases, so that if you are turning up, you know, touch accuracy problems, it

doesn’t matter where that happened, we should be taking account of it. I think what we need to do is get the test protocol people together to really work out the details.

DR. JEFFREY: If I could interrupt. I don’t think we are going to actually develop the test tonight no matter how much I think all of us would love to.

David, I would just like to remind you that forty-five minutes and then thirty minutes tomorrow and you have hit the first of five topics. So if you could focus down, that would be great. Thanks.

MR. FLATER: Well, I don’t have a button that means go back to the top. Alan can you put be back on slide one real quick? I just want to go to the top really quick.

Given that we have limited time will the committee care to express a desire as to which topic it would like to hear about next?

DR. JEFFREY: Let go to COTS unless anyone has –

MR. FLATER: Put me at the beginning of the COTS presentation please.

COTS arguably is an issue on which we have seen a higher than typical level of consensus going on among CRT and STS which is surprising given how contentious the issues seem

to be at first. There was a resolution passed way back in the dusty early days of the project that seemed to express the sentiment COTS considered harmful in so many words.

This resolution was motivated by some concerns. First of all a belief that COTS is automatically exempted from scrutiny by the test lab and this combined with concerns about “rotten COTS” that is not suitable for voting use combines to create a large worry that rotten COTS plus never tested equals bad system.

Upon closer inspection these concerns essentially weren’t borne out by reality. Even looking at the current standard, although many people clearly believe that the current standard exempts COTS from any kind of testing, I did not find evidence for that interpretation in the standard itself.

The guidelines are confusing on the subject of COTS and in places possibly even self-conflicting, but COTS is not exempt from test lab scrutiny. A part of this confusion, I believe, results from terminological limitations, trying to characterize everything as either COTS or not COTS. It ignores a lot of boundary cases that have come up, continue to be raised as interpretation issues.

Furthermore we can observe that something close to a ban on COTS would seen to be what the resolution originally was thinking about, ignores the reinventing the wheel effect. If in fact there is a good COTS product that satisfies a particular requirement, it can simply be incorporated that this may be a preferable approach to designing the system than trying to reinvent that wheel. So, having discussed this on STS calls and the resolution was originally and STS resolution, the consensus I saw was that in fact, yes, moving forward the way I'm about to describe was actually a satisfactory reaction to the resolution. I will leave the question as to whether a motion to amend the previously adopted motion is necessary or not.

This table shows a summary of the different categories of software that have been split out from simply COTS and non-COTS and the applicable levels of test lab scrutiny that they would get. At the bottom we have COTS and I'll be going into the definition of that but COTS is essentially that for which we cannot reasonably demand to receive source code and expect to get it. That does not mean we cannot test COTS.

You can always test a black box. You give it input

and you observe the outputs. You can conduct black box testing on COTS. You simply can't conduct those portions of the test campaign that require you to have source code.

At the next level we have clear box testing. There is an assortment of things in here. The border cases if you will. These are things for which its not reasonable to impose coding standards because, for example, these are things that aren't in a programming language to begin with or are constrained by their application such that they cannot conform to coding conventions.

The third level we have most of what is currently done with voting system application logic. The software at this level is not only subjected to black box and clear box testing, its also reviewed to see if it conforms with the coding standards which are intended to enhance the readability, maintainability, etc. of the software.

At the highest level we have a new concept, logic verification. It is applied only to core logic and I'll be describing what that is, a subset of application logic. Its actually another one of my presentations. It goes into detail about what exactly it is and what the ramifications are.

In a nutshell, I would say don't read too much into the column title that says Shown to be Correct because I agree totally with what STS said earlier, if you are looking for one hundred percent assurance that software of any reasonable complexity does a particular thing, you are not going to get it.

Given certain compromises, we can talk about logic verification giving a higher level of assurance than what we can get through the current testing. If not a high enough level of assurance to satisfy some of the security requirements.

On slide 58 which may or may not map – does that map to the page numbers you have? Good. Okay.

Slide 58 has a definition of COTS. Software, firmware, device or component that is used in the United States by many different people or organizations for many different applications and that is incorporated into the voting system with no vendor or application specific modification. Yet, again, very carefully written, legalese definition which probably completely fails the plain language test, but it currently captures what we are capable of capturing with regard to this definition.

I'm going to come back to this later. There have been discussions about making a more precise definition to put here. Essentially we are removing the assumption that COTS is in fact commercial software. Keeping the term COTS because its easily recognized by everyone, but, in fact, even though COTS stands for Commercial Off the Shelf this may well be an open source package.

Application logic which is what gets the coding standards is software, firmware or hardware logic from any source that is specific to the voting system except for blur logic. Core logic which gets the highest level of scrutiny is the subset of application logic that is responsible for vote recording and tabulation. The assumption here is that you have literally a core of logic that has been designed into the system to do these highly sensitive tabulation operations and that the user interface or interfaces, device drivers, etc., all these additional pieces of the system surround that core.

Finally, for the clear box testing level we have all the extra and exception cases. Border is one of the cases that's come up in practice. Its defined as software, firmware or hardware logic that is developed to connect application

logic to COTS with third party logic. For example, when folks are using a COTS database package it requires you to integrate with the database using a particular database language which is not necessarily going to satisfy the coding standards and the guidelines. You want to design the system so that this special requirement for this different language and different coding standards is wrapped, if you will, is isolated from the part of the system to which we can apply these other levels of scrutiny but border logic is exempt from the coding standards.

Configuration data is fairly commonsensical, non-executable input software, firmware or hardware logic. There have actually been questions of the form, does HTML have to conform to the coding standards because someone was either worried or had already been asked to do this, that somehow the standard could be interpreted as mandating that coding standards intended for a programming language be applied to something that is a mark up, layout and display type of language.

Finally under clear box testing we have third party logic. Once again we have not very easily pronounced definition. What it boils down to in plain language is,

things like Windows CE, things that look like COTS but aren't because they are not widely used or generated code. This is the grab bag of other things over which we just don't have enough control to say that these must conform to the coding standards but you still must deliver the source code.

The concern about rotten COTS, in fact is a non-issue. COTS is not automatically excluded from anything except the requirement to deliver source code and that's for pragmatic reasons. Having received this system to be tested the test lab must make a determination whether previous certifications and field experience render any portion of the test campaign redundant.

This is a global concern. If you get a piece of equipment that has been previously certified as an FCC class A device, whether its COTS or otherwise, you are not going to rerun that test. They have go the certificate right there. So the test lab always has to make this determination of whether some part of the test campaign is redundant. If, in fact there is a piece of COTS that arguably has already been demonstrated to satisfy the requirements of the guidelines and is suitable for use in voting systems, etc. that would feed into this determination.

However, any reduction in the scope of testing must be justified in a test plan and approved by the EAC. So this is a controlled process. Nothing is going to be automatically excluded from scrutiny. If we do have " rotten COTS" it will not have demonstrated itself as suitable for use in voting systems in practice and it will not qualify for reduced scope of testing.

MR. SCHUTZER: There are a couple of things that we had discussed in our calls regarding COTS. First of all one thing as you pointed out if its open source like Lennox or something and its not out of the question that you might require the source code since it is available in that instance.

I think the other thing that we discussed was that, which is common practice in a lot of financial services firms, etc. is that part of the problem with COTS is, of course, it's a general purpose thing that has lots of flexibility, lots of different capabilities and so forth. Its good recommended practice to turn off and cut out a lot of that part of the software which could get you into trouble which is not really needed for the purpose for which you are talking about.

So, we are talking about a DRE that's going to have any kind of communications capabilities and is going to be using JAVA script or a variety of other kinds of functions you would want to turn that stuff off. Lots of different interfaces and IO that will get you out of a lot of trouble in terms of you might even have some recommendations for different classes of COTS, what it actually gets when its configured and eliminate it from the package.

MR. FLATER: I acknowledge that is a serious issue and concern and particularly with respect to COTS where, since it hasn't been designed specifically to voting system requirements its bound to come with some parts that aren't used and what are you going to do about those. Yes, we should discuss that more. Certainly, STS, I believe, at various times has made recommendations to the effect that, well, if its not used then its just a security risk, get rid of it.

MALE SPEAKER 31: My question is the same. What are the specs for black box testing for a COTS product where you are only using a piece of it? Who develops the specs?

MR. FLATER: Well, at any rate its going to be tested as part of the complete system.

MALE SPEAKER 31: Sure, but you are talking about separately testing the COTS product here, black box testing, is that what this means?

MR. FLATER: I won't commit strongly to that. It may suffice to test it as part of the complete voting system because really what you are concerned about is how it performs as part of the system.

If there is a need for more focused testing of just that part of the system, that's something we need to discuss further because off the top of my head I don't see a strong case for it. From a security point of view it may well be necessary, I don't know.

MR. WAGNER: I have a question probably because I'm new here. One concern I've heard raised about COTS is the malicious code or the Trojan Horse concern that the COTS might have a malicious logic hidden somewhere in the source code.

One thing to note from the security field is that you, generally speaking, cannot detect those kinds of Trojan Horses using black box testing alone. So the concern would be that testing labs might be unable to tell whether or not that was present given the current regime here where they

would only be doing black box testing because they don't have access to the source codes.

If the outcome of your election is dependent on the correctness of the software then malicious logic in COTS code might be a problem because it might go undetected.

What's the position that the VVSG or the CRT is going to take on that? Is there one?

MR. FLATER: Well, presently everything I'm presenting is discussion points. This is a topic on which I should defer to STS. Off the top of my head what I see, if we verify that in fact this is genuine COTS, meaning this is a general purpose package that was not developed specifically for the voting system, we have generated some confidence that if in fact there is a malicious Trojan Horse in there, at least its not one that was customized specifically for the purpose of throwing elections unless there was a very large conspiracy.

MR. SCHUTZER: That's part of what I was getting at when I talked about some guidelines you might want to have on COTS which is to say that, not the issue of someone actually trying to insert something, customized as he said, but if you were to say that I have a PC and from the day I get it

and the day its configured, first of all its stripped of a lot of capability, its never, ever used to read in new discs and new software, other than the procedure by which I put in the software for this one single application. Its never, ever used to go on line, I think I have eliminated an awful significant source of any Trojans. You could probably be fairly confident that you are not going to be in the same position as somebody who is actually using their PC to actually surf the web, do internet and do a variety of other things.

MR. WAGNER: I'll just comment, I don't see why, on what basis we can reject, why it would require a large conspiracy or why we think its unreasonable, impossible that someone could insert malicious logic that's customized for voting. Even if its used in other applications, it seems like the conspiracy size might be one and if its public knowledge that that COTS is indeed used in the voting system, you could imagine the maintainer of that package inserting malicious logic that's customized to attack a voting system. I don't see how we can rule it out.

MR. SCHUTZER: Yeah, but that's the same issue as somebody in the application logic doing it, the same threat,

which you address in the same way in terms of software independent verification.

MR. FLATER: It's a similar issue. The threat level, the risk is increased if we are talking about COTS because we're not talking about just one vendor but now we may be talking about many vendors if the voting machine assembles COTS code from a number of vendors.

On the other hand that exploit would have to somehow be interoperable with all of the different vendors application logic in order to actually, effectively allow you to throw the election.

If we are talking about the one person at the operating system house trying to put a bug in the operating system that the vendors are using to allow that one person to cast fictitious votes on election day. That malicious logic would have to know enough to interoperate with the different vendors' products well enough to actually make that happen. Its much easier, I think, to envision a conspiracy of a size of at least two, in which that person talked to a vendor to get the internals or a rogue person at the vendor to get the internals necessary to rig that up. I'm really way out of my depth here. This is something I should defer to STS

to talk about.

DR. JEFFREY: Maybe we should continue this a some other forum.

MR. FLATER: So we may not have consensus on the notion that the rotten COTS issue has been dealt with.

(END OF AUDIOTAPE 4)

* * * * *

(START OF AUDIOTAPE 5)

This suggestion came out of STS, a very simple way to answer this question is to have the test lab obtain the COTS pieces independently and either integrate or witness their integration into the equipment to be tested. Witness integration is more likely a scenario than integrate as long as the test lab has independently gotten its COTS the vendor asserts is compatible the system. It seems to address this concern in a very nice, neat fashion.

Among the unfinished business and in addition to the discussion we just had, there was discussion about coming up with a more precise definition of COTS that was inconclusive but it included the notions of publicly available, widespread use, possibly quoting a benchmark of the number of deployments. The requirement for the

maintainer too have existed for some number of year and also a requirement for proper configuration management.

It's the middle two, the two with the benchmarks that have unresolved issues that we never reached an end of the discussion on. With regard to the widespread use, its not always possible to verify the number of deployments with respect to the longevity of the maintainer, we can envision many scenarios in which companies are bought and sold and the way that this happens there is no particular mapping to life cycle of software itself or its stability or even how well maintained its going to be.

MR. SCHUTZER: What's the purpose of this kind of a definition? Other than the simple one of saying its something I can buy off the shelf. The only reason I can think of a purpose for this was which stuff I can buy off the shelf would I not permit to be used. That might be something where maybe its of such a small distribution as to be more viable for someone to insert an attack as contrasted to David's comment to you that if its in very wide use and you've got lots of different moving parts and pieces by lots of different vendors, it going to be pretty darned hard for somebody unless he gets into the application logic of the voting to defeat

it, unless you are talking about some Trojan that's coming in because I'm using it in general surfing matters.

I think we ought to understand a little more why you want to have a definition more constrained than off the shelf. I think the market will determine its something that is a very limited distribution and use is not likely to be picked up because its going to be not very attractive.

MR. FLATER: To answer this question I would defer to the origins of this definition which was some combination of Ron and Steve.

MALE SPEAKER 32: Maybe I could comment about exactly what off the shelf means these days. I mean if you are talking about something that you pay for that's one thing. If you are talking about stuff you download from the web, that's a big shelf out there and there's lots of stuff on it.

MR. SCHUTZER: But the purpose of our defining it is for what purpose? What COTS we would include and what we would exclude from being allowed?

MALE SPEAKER 32: Its what you said earlier, trying to exclude –

MALE SPEAKER 33: Stuff that's too small to be

plausible. It says either used widely enough to be developed independently –

MR. SCHUTZER: Okay, so I could buy that. The last thing you would want to do is pick off something that just happens to come off the shelf that looks pretty darn attractive because of its functionality and it turns out some nefarious guy that's put up this very attractive thing for the sole purpose of infecting – here's a nifty, difty (undecipherable) that you might like to use.

MR. BERGER: I might like to add to that discussion quickly, we also had some conversation there about having some assurance that the generic use of the COTS was sufficiently close to the use in the voting system that there would be some confidence that in fact it was fit for use.

MR. FLATER: Another idea that came up in the discussion of COTS was that there is an opportunity that the EAC could maintain a list of COTS products that were previously found to have been acceptable for use in voting systems. This would be input into the determination of a test plan that would still be the work that the test lab would have to do to ensure that the use of the COTS product in a new system is comparable to its use in the previously

approved system. If that's not true then nothing from the previous approval would be applicable. In any case there would be no waiver from system testing, you always test the entire system.

MR. SCHUTZER: That could get around some of the concerns while you struggle with the definition. If you can only use COTS from a finite list that you have there and then that sort of closes the universe to what's acceptable.

MR. FLATER: So, that's the last slide in the COTS presentation. Are there any additional questions or comments on that one?

We have just less than twenty minutes left in the day. Rather than try to scroll back to slide one I will ask you among the remaining presentations we have –

DR. JEFFREY: David, let me actually rephrase the question to you. Which sections are absolutely critical in terms of getting input for your continued work? Which do you need input from us on? You've got conformity assessment, scope of testing, coding conventions and logic in California volume reliability testing.

MR. FLATER: The issue on conformity assessment,

scope of testing, I already know from the last CRT call is quite contentious and we don't have a consensus on that and I think if I brought it up now we would simply argue for twenty minutes.

Coding conventions and logic verification is actually – the direction has not changed from what was given, if you will cursory approval by the committee last year. However, there continues to be a lot of concern about that. So, perhaps I should present that.

If you just put that full screen then we are ready to go. Okay, just over fifteen minutes.

As I said, this hasn't changed since September 2005. Coding conventions are requirements on the form, not the function of source code. They are, some of them are requirements affecting software integrity that have been implemented as defensive coding practices such as error checking, exception handling and also prohibitions on practices that are known to be problematic.

The current direction that everyone seemed to be okay with as of September 2005 was to expand the coding conventions addressing software integrity which I would describe as the twenty percent with eighty percent impact. Clarify length

limits because these are necessary to keep the code intuitive enough to do the logic verification but delete the eighty percent of the coding conventions that only have twenty percent of the impact on software integrity. There have been problems with those that have been incorporated into the standard have suffered from rapid obsolescence because the state of the art advances faster than revision cycles for the standard.

Instead what we would like here, instead of putting specific prescriptives conventions in the standard for these kinds of stylistic issues, require the use of what are essentially the current best practices. The old standard used this formulation of published reviewed, industry accepted sort of a vague collection of words. The new vague collection of words is published credible, although there are definitions for what these mean that try to help.

Once again, as with COTS there is an opportunity here. Rather than rely on these problematic definitions in the standard, they are very hard to nail down very precisely. The EAC could do an end run around that whole issue, have a process to periodically review current best practices and publish a list of coding conventions that are acceptable

for use in voting systems. That's an opportunity and its hard to say if it will come to pass.

Now the most controversial aspect with regard to the coding conventions is the requirement to use a language that has block structure exception handling. Block structure exception handling to any programer who is present, this just means track (undecipherable) statements like that.

Most of the languages are in popular use these days already have this, but there is an issue which is one very popular language doesn't have it and that is the C language.

So there is some concern that inasmuch as there is some investment in legacy code that is in C and inasmuch as if this code is recycled as part of a new system. It would be certified under the new standards as a new system that C code would have to be migrated. In fact this migration shouldn't be that bad because there are three descendants of the C language, all of which do have block structured exception handling, JAVA C++ and C sharp from which the vendor could choose to conduct the migration of the code. There is other alternatives that could be used if in fact this were a system to be built from the ground up.

The case for exceptions was made as far back as 1989 and we know that it goes back farther than that because block structured exceptions appear in the AITA (sic) language in 1983 and, I believe, in some semblance possibly prior to that. I'm not sure.

I'm going to quote from an author from 1989 that puts it very succinctly, "one of the major difficulties of conventional defensive programming is that the fault tolerance actions are inseparably bound in with the normal processing which the design is to provide. This can significantly increase design complexity and consequently can compromise the reliability and maintainability of the software."

So there is that argument for why block structured exception handling is good. There is its general acceptance in programming practice now and there is the fact that the voluntary voting system guidelines require recovery behaviors that are nicely implemented using block structured exception handling. There are all the forces combining to suggest that this is an idea to think about.

MR. SCHUTZER: So, again, considering that we are talking about the next iteration philosophy, why wouldn't

we just want to be done with it (undecipherable)?

MR. FLATER: Its simply a matter of its change. It would be a mandated change and somebody whose system is entirely in C code would have to react.

MR. WAGNER: I have to admit that I do have some concerns about that. Again, I'm new here so I probably missed the previous discussion. There are good reasons why operating systems and imbedded systems are often written in C instead of, for instance, C++ or these other higher level languages, so there is some burden here. I wonder whether its really necessary to forbid C to get the good things you want.

There are ways, there are extensions to C, software packages that can provide structured exception handling. Its your Windows program or you may be familiar with SCH structured exception handling which provides in C the ability to provide this feature that you are looking for. There are also other non-proprietary implementations as well.

So, I wonder whether its really true that this new requirement actually does rule out C. If it does rule out C, I think the cost of that may be very significant.

MR. SCHUTZER: I just want to get some clarity. Were

you just referring to the application program that gets built on top of various COTS components? We're not talking about actually systems that build their own operation systems yet, are we?

MR. FLATER: No, this applies only to those portions of the system to which the coding conventions apply.

MR. SCHUTZER: Right. So, --

MR. FLATER: But to answer what you said, what you described is a credible path. Instead of saying you must migrate to a descendant language such as JAVA C++ or C sharp, saying it would also be acceptable to use one of these extension to the C language. I think that would be okay.

I would accept that, I suppose, as a friendly amendment to the direction if no one has a problem with that.

MALE SPEAKER 34: Just to make clear what you would be recommending is having block structured exception handling and not putting a requirement to us to how one gets there.

MR. FLATER: Yes. It needs to be thought about. I need to look at and do the background work on these extensions. I've seen one already. It was just someone's hack so I need to find the good ones and convince myself

that there really is a solid state of the art here in terms of retrofitting C as opposed to migrating.

I'm not sure that it would be less effort, I don't know. The kind of changes you have to make to the code might be comparable but certainly I accept that this is not something to rule out at this time.

Okay, eight minutes. Logic verification. Don't panic. Its not what you think. Logic verification is formal characterization of software behavior. I've already started adding caveats within a carefully restricted scope I'm talking about.

Generically speaking its proof that the behavior of the software conforms to specified assertions, i.e., votes are reported correctly in all cases. It complements what we call falsification testing or typical kind of operational testing which, as I said earlier, if you get an example of misbehavior by the system you have proof that the system doesn't conform but if it happens to work in the specific case you tested, you don't know that its going to work in all cases.

Logic verification tries to do an analysis of the source code to generate confidence that it will be correct in all

cases.

The motivation for this was a TGDC resolution asking for a higher level of assurance in operational testing alone. Also to clarify the objectives of the source code review. We don't just care about coding conventions for stylistic reasons, we also want to be able to do this kind of analysis on it.

The way this would work using a traditional inductive assertion sort of approach, the vendor would specify pre and post conditions, logical conditions for each callable unit. The vendor would prove certain assertions regarding the tabulation's correctness. The testing authority would review this analysis and find that, if everything is okay, the pre and post conditions correctly characterized the software and, that assuming those are correct, that the assertions are satisfied.

Now, we have said already, earlier in the day, that doing this kind of proof on complex software for non-trivial properties is, for all and intents and purposes, impossible. Compromise number one is that the scope of this will be limited to core logic which as I said earlier is the subset of application logic that is responsible for vote recording

and tabulation. The user interfaces write out.

It would be really nice if we could show that votes aren't being defrauded in the user interface but if we set a scope of that size, this simply won't be doable with the kind of resources that are available.

Compromise number two is that we are not even doing this with the level of formality that we would like. Given that the programming language itself does not have formally specified semantics, its very difficult to carry this through into a formal proof. So, what is feasible is to use formality where possible, otherwise use informal arguments and rely on the limitations on complexity meaning length limits on callable units to make the correctness of those assertions intuitively obvious. Question?

MR. SCHUTZER: What are you really talking about now? We are not talking about formal proof, we're talking about what, code inspection and convincing ourselves that there is no logic errors in there by just reviewing it?

MR. FLATER: Its in between that. We are going to have an argument separate from the code itself, as formal as possible, certainly logically valid, about the correctness of the code. Its not going to be at the level

of rigor as a formal proof to really show with one hundred percent confidence that its correct.

The bottom line here, is as Boris Bazer (sic) in one of his testing books, “if you want to get quality code, you must read the code, read the code, read the code.” So this exercise, while it will not achieve the lofty goals that are usually the target of logic verification, simply performing this exercise will give us a higher level of assurance in the code than operational testing alone.

This could be attacked from both sides. Its too rigorous. Its too much work. Its not rigorous enough because you didn’t prove anything. Its too complicated. We need people who are trained in logic to do this. Actually its over simplified using an informal proofs. They don’t prove anything. Wait, this kind of analysis is only appropriate for safety critical systems. They are the only ones that have the resources to do it. This is a pale imitation of what is done for safety critical systems. Why are you even doing it?

Some people think that consensus is that middle position which causes both sides to be equally angry with you. This may be something we could reach consensus on. I think it’s

a pragmatic proposal.

MR. BERGER: David, a point of clarification and then a question. A couple of times in your wording I haven't been sure whether you were talking about formalistic verification formally or formally and specifically there's work in several areas about formal verification of software, JAVA II platform and so forth. What's the applicability of those kinds of approaches especially to the nucleus core logic that we have in voting equipment?

MR. FLATER: I'm not familiar with the JAVA II platform verification that you cited so I don't know.

MR. BERGER: How about just the whole approach of formalistic verification of software?

MR. FLATER: Well, the basis, the beginning of this was looking at inductive assertions using pre-imposed conditions. Is there something else that you mean?

MR. BERGER: I think so, but given the hour, why don't we take it off line.

DR. JEFFREY: Any other comments or questions for Dave? Got a couple of more hours to go tonight. So, anyway, thank you Dave. No shortage of work there. Again, tomorrow, you have two different topics that you haven't hit upon.

If there is a way of, thinking about it overnight, how to shrink it down to thirty minutes, so that we can reasonably stay on schedule.

That was great. Thank you and to all the other briefers today, I think there is no shortage of information.

Before we break if I could just make one observation. In the very, very first slide that was shown today where Commissioner Davidson showed the schedule, if you notice that on July 31, TGDC should forward the draft VVSG to the EAC. So that's, given that December not a lot happens, that's seven months to complete all of that to get to the draft.

If we end tomorrow with a lot of open issues, we are not going to get there or we are going to have a lot of open issue come July. There needs to be enough time to do the analysis, to dot the I's cross the T's and then to make sure that the end product is actually something that will meet all of the needs of all of the constituents. So, I urge you as you are having dinner tonight, to think about some of the things that we covered today, to think about additional open issues and see how many of those that we can close tomorrow to provide the guidance necessary to produce a really good draft by July.

Are there any other last minute comments or questions? If not, thank you very much. Notice that the schedule shows us starting tomorrow morning at 8:25. So, see you bright and early.

Thank you all in the audience for your patience today.

(**END OF AUDIOTAPE 5**)

* * * * *

CERTIFICATE OF AGENCY

I, Carol J. Schwartz, President of Carol J. Thomas Stenotype Reporting Services, Inc., do hereby certify we were authorized to transcribe the submitted cassette tapes, and that thereafter these proceedings were transcribed under our supervision, and I further certify that the forgoing transcription contains a full, true and correct transcription of the cassettes furnished, to the best of our ability.

_____

CAROL J. SCHWARTZ

PRESIDENT