Technical Guidelines Development Committee
Plenary Meeting 3/22-23/2007
Captioning Text: Day One

This is nist, this is the teleconference phone line for the 9:00 meeting. Is anybody online?

Could we all start to take our seats so we can begin.

Good morning, everybody, I just want to take a check here first to see if the tgdc members that are online can hear us, and they could hear them. Could you so identify us, if you are on the teleconference. Sounded like someone was just on.

Good morning. This is phillip pierce.

Good morning, this is alice miller.

Thank you, alice. Anyone else? I'm assuming you both can hear us and we'll identify people as they join us. Good morning, everybody. I'm allan eustis with the nist information technology laboratory, welcome to the 8th plenary session. Just some quick overviews we would like to do we are now located in the employees' lounge. We also have an overflow room in lecture c. If we have a fire or fire drill or emergency, you'll hear the sounds and be warned and here is the exit. You go out the door here, and take a right, and keep going down the hallway, and you can see the glass doors. From lecture c you want to go down the hall to the right and down out the entrance. The main entrance is the faster way there. There's a lot of rf in this room as it is, so it would be helpful if you turn the cell phones off. It's best not to have food, but I'm already violating that with my cup of coffee, so I probably can't tell you not to do that. Please-- please wear your name badge while you are here. If you are planning on coming back on day 2, and you are driving, if you bring your name tag and license identification you do not need to go back through the security shelter. And we'll meeting here tomorrowing starting at 8:30. We'll be breaking for lunch at around 12:30 and the cafeteria is right across the way here, so with that, welcome to gaithersburg on a nice march day. And Dr. Jeffrey the meeting is yours.

Thank you very much, and since I'm violating it rule no. 2, I guess I'll waive it for everyone else. So first of all, good morning, and everyone welcome. I'm william jeffrey director of nist and chair of the tgdc t, and I here by call the 8th plenary session of the tgdc to order. First, I think we should stand for the pledge of allegiance. [pledge of allegiance recited]

At this time I would like to recognize brand new parlimentarian for the tgdc. Ms. Thema alan who will now do the official roll call.

Okay. Williams? Williams not responding? Burger? Burger? Burger not responding. Wagner.

Here.

Wagner is here. Paul miller? Paul miller? Paul miller is not responding. Gail? Gail? Gail is not responding. Mason?

Here.

Mason is here. Gannon.

Here.

Gannon is here.

Pierce?

Here by teleconference.

Pierce is here. Allapse miller.

Here.

Per sell?

Here.

Per sell is here.

[indiscernible].

Here.

Vest is here.

Shooters?

Here.

Turner billy?

Here.

Turner billy is here. Jeffrey?

Here.

Jeffrey is here. We have 11 in attendance that is a quorum.

We have our signers over to my right, if anyone needs their services they will be here this morning and this afternoon. And please find a seat over here on the right side.

Thank you. I'll mention I know a couple of the tgdc members are stuck in various airports due to bad weather in the midwest and they hopefully will be here within a few hours. I again, would like to welcome everyone back to the and to the gaithersburg campus of nist. I know everyone has been working very diligently and very hard over the last several months so we have got a lot of work ahead of us, before we get to the next it ration of the tgdc guidelines to the eac on schedule in july of 2007. And we have really benefited from the advice and counsel that has been provided by this body, so I really do look forward to the next few days of continuing that as we try to wrap up and get sort of a little be it of the finishing product going. I'm especially pleased to representatives from the eac this morning. Commissioner davidson-- is commissioner hillman here? Okay. I think she eel be here later. And two newly confirmed commissioners who will join us shortly. And I would like to welcome back tom wilky and his senior staff who have been an absolutely invaluable help

to us. At this time I would like to entertain a motion to deposit the minute from the december 4th at 5th tgdc meeting is there a second? There is a second. Is there motion for unanimous consent-- I'll call for unanimous consent, any objections? Hearing no objection, they are accepted. So also we have to entertain a motion-- we missed the minutes from the last meeting, I guess. The march 29th meeting of the tgdc committee. I'm sorry the-- so much in my notes. So the agenda for this meeting we need to adopt. Sorry my apologies any second? Okay. There's a second. Any objections to unanimous consent? With this formal lizment we now actual I will have an agenda. Since the last meeting in december of 2006, the three working subcommittees of the tgdc have drafted and edited sections of the next it ration of the vvsg. They are be reporting back at this meeting. Specifically as a committee, we will review, approve, and where appropriate, provide supplemental direction to the subcommittees. This is guidance is critical to the refinement of the final guidelines that we'll hand to the-- tgdc members highlighted the immediate for subcommittees to collaborate on issues of mutual concern, and we're going to discuss the results of those collaborations tomorrow. Now the time required for us to actually go through this agenda means that the committee cannot take public comments at that meeting. However, there are opportunities and will be continued opportunities for the public to comment. In fact, I would like to emphasize that point; is that the documents-- the draft documents are on the web and are available for users, vendors, or public, if you have any initial feedback, please email us, we'd be happy to accept that. In addition, I would like to mention to additional things that we're going to be doing, as we get closer to handing over our draft guidelines to the eac in july, we want to make sure that those guidelines are as good as possible; that we have captured as many of the needs of the community, and that they are attestable, and are drafted as-- as well as could be done. So what i'm asking is that for each of the three subcommittees, i've asked that there with be co-chairs to each of the subcommittees where this co-chairs will be venttives of the end users, people out in the states and localties who have to make sure this implemented. And paul miller has volunteered to be co-chair on the core requirements team. Allapse miller has agreed to be co-chair of the human factors and privacy team, and alan p, rsell has agreed to be on a subcommittee. Thank you for your work, and again, I want to make sure we don't have any gaps in what we mutt forward. Along those lines an important component is when we have the guidelines that they need to be testable and verifiable as they get implemented. And whitney has discussions with us, and so what I have asked since navlab works under nist, I have asked them to start participating in the subcommittees to ensure the guide lances are drafted in such a way in to something that can be tested and verified. So I want to make sure we don't have some inconsistencies across that boundary. So the navlab folks have agreed to that any additional comments, position statements about the work of this committee can be sent to voting at nist.gov noting at nist.gov, and they will be posted on the website and comments we received today are already posted there and will be reviewed by members. At this time it's my great pleasure-- and let me just mention that commissioner hillman has joined us. Welcome and perfect timing because this is the opportunity now I would like to invite both commissioners to address this committee. I would like to-- [indiscernible] .

Good morning. Well I want to start by thanking each and every one of you sitting here today and on the telephone for the next two days and all the time that you have served indefinitely giving your guidance in this extremely important task, and your opinions is a valuable in this process, and we really do appreciate it. Before I start, I think-- well maybe I better go ahead and then I'll introduce them if they get here before I finish. Commissioner hillman has been introduced, and as you can tell, she will speak right after me. She's going to inform you how we're going to start getting our boards advised with this process so we have

them definitely educated as far as we can-- because they are a real important part of this process. As we begin your meeting here trade and begin to discuss the next it ration of the vvsg, I think it is important to note where we are in this process and where we have to go. You have worked hard since the 2005 vvsg getting to where we are at today and after the deliberation of the next two days, nist and the leaders of the tgdc are looking to hold another meeting in mid-may. To finalize the details that will be coming to us, which is planned july of '07 to be delivered to the eac. The delivery of the tgdc draft version is an extreme I will important step, but it only marks the beginning of the next part of the process. After reviewing the tgdc draft, the eac has the responsibility and mandated under habba to conduct a deliberate and thorough review of the document. First eac will review and-- the tgdc document it's a. Second-- publish their draft version in the federal register and receive public comments for a minimum of 90 days. Also, the habba requires the eac board of advisors and standard board get a minimum of 90 days also to review and give comments. After the close of the comments, the eac staff must review, catalog, and incorporate the comments submitted by the boards, by the public, and by all members that have interest in giving these comments. For the 2005 version, I think you have heard me say it before we got over 6,500 comments that had to be vetted, and we worked very hard along with nist to make sure that we were-- had the very best product we could have at the time we adopted the 2005 in december. This was only a partial rewrite. This time the vvsg is a complete rewrite. So amongst-- with the steps of habba requiring eac, it always has this holding public hearings to meet with our stakeholder. For instance we need to know what is the election officials need from the marijuana sheens? We need to know thoughts and concerns from advocacy groups. We must engage the voting system manufacturers to understand the technology available and the time line for development. This includes an open and honest discussion about how much its going to cost to develop, manufacture, and test. In order for these guidelines to be functional, they must be affordable. The point of all of this is that the next it ration of the vvsg is going to take time and to do it properly it should take time. Unlike the 2005, as I said, h this itter ration is a complete rewrite anything short of a methodical, systematic and thorough review by the eac is irresponsible. With the support of nist, it is our goal to create a set of standards that won't need to be looked at again for four years. Eac's goal is to end the cycle of constant change between elections. The creation of comprehensive set of guidelines is the only way to accomplish that goal. Vvsg is-- is only one element in the process, though that we have to consider at the eac. Elections is more than just the machines. We have been working hard in conjunction with the vvsg to make sure that our election management guidelines aid the election officials in administrating the most transparent, accessible and trustworthy elections possible. For the vvsg ends off the technical guidelines and the management guidelines were-- the technical guidelines in the-- the management guidelines begins. In taking the best practices and advice on the administration of elections. Currently the eac is working on five new quick-start guides for the officials. These five guides will cover: election certification, developing an audit trail, public relation, disaster planning and change management. The goal is to relieve all of these prior to the 2008 elections. So the fall-- we would like to have everything out by september of this year. In conjunction with the management guidelines, the eac is working to develop several new chapters in the management guidelines. These new chapters will cover everything from military overseas voting to polling place management and also mail and absol lent tee ballots-- the election center-- and we have offered this to other election training areas, is going to hold a meeting in-- in kansas city in april, and that meeting, they are introducing a lot of our management guidelines. In conjunction with all of this is obviously what is our top priority for 2007? It is to increase public confidence in the election. To

achieve that goal we must increase voter confidence in voting equipment and the process. The means-- that means a vigorous system of testing and certification of the equipment, educating the public and the voters about the process, and continuing to examine the way we conduct elections and making improvements as we go. So we have a huge job ahead of us, but we're confident that we can meet that goal with all of the help that we have in-- in our group that we are working with. I want to tell you how much I look forward to the next two days in learning everything that's coming forth, and let's see if we have the new commissioners here yet. No, but when we do, we'll make sure that they are ber do you seed. Thank you very much. I appreciate it.

Thank you very much.

Good morning, everybody and thank you for the opportunity to be with you this morning. As commissioner davidson said we are appreciating the normty of the task before us over the next several months to perhaps a year to get through the next iteration of the voting system guidelines. Perhaps the two biggest challenges we have are helping our standards board, our 110 member standards board and our board of advisors prepare for the roll that habba mandates they perform in reviewing and commenting on the guidelines, but beyond that we have got to undertake the task of helping the public digest what we are doing. And I think a predecessor to that is to make sure that even among the groups that are intimately involved and familiar with the vvsg, that the scientists and the technical experts and the election officials can communicate and speak the same language, and quite frankly we're not so sure that is happening right now. In response to that, the standards board is starting now to prepare for its work, and we will be joined today by one member of the standards board, who was serving on what is being called the vvsg ad hoc committee of the standards board. And basically that committee consists of three members of the standards board, but in a very short it will grow to larger-sized committee this ad hoc committee will work with the executive board of the standards board to really review what its task is, how to help the standards board members receive the information in small enough bites that they can adequately chew and digest it before getting to the full main course after the recommended guidelines are ready for public comment. And I expect that the board of advisors will be doing the same thing, and the board of advisors subcommittee and the standards board ad hoc committee will be working together over the next several months to accomplish this. And in many ways they are important spokes people about this subject in the states to the more than 7,000 election officials-- state and local election officials there are in this country, as well as to the grass roots community. As we know the public has never been more interested in the very specifics of how voting systems work than they are today. Irrespective of whether the issue is access, accessibility for persons with disabilities, security, you know, functioning, human interaction, whatever the situation might be. So we certainly want to make sure that those two important resources are adequately prepared to have discussions in their communities with their county officials, state officials, governors, whoever it may be to help everybody appreciate the implications of the volunteer voting system guidelines on the future of voting and democrat in america. And thank you so much. I look forward to the conversations as well.

Do we have bill campbell. All right. He is here. Please let me introduce bill campbell who is the city clerk from the city of will burn, massachusetts. He has been a member of the standards board since it was organized in 2004 and has just completed a tenure on the executive board. He's here for the two days to observe, and will be an important reporting mechanism back to the executive board. Thank you.

Thank you very much. Definitely appreciate the absolutely strong support and good working relationship that this committee has had and we appreciate the comments from the commissioners. At this point, I'll ask mr. Mark skall to review summary of activities since december 2006, and I believe all of that information and his briefing is contained in the three-ring binder marked workbook. I will also reiterate one of the comments that commissioner hillman made. During these presentations the closer to english we can get, some of the technical briefings, the better we will all be served, so with that challenge, mark.

You know, someone from book listen, new york that's very difficult to meet that challenge. Good morning. I would like to tell you about the voting activities that nist has been engaged with over the last few months so this an overview of what i'm going to speak about. First of all, since-- since december 4th and 5th, which was the last tgdc meeting, we have been very, very busy. As you know the tgdc itself makes recommendations to the eac with respect to volunteer voting system guidelines. Nist, of course, provides the research and actually drafts the words that go in to the vvsg. We of course cannot do this without very close coordination with the tgdc. Outreach is a very important air glachlt doing our research we want to make absolutely sure that we meet with everybody we can meet so we understand the environment we're working in, so that our research as a thorough as it can be. Those of you who have been involved with the tgdc from the beginning know that from the first iteration, during this iteration, we really are trying as well as we can to reach out to as many different people so we can learn everything we can in order to do your research. Lastly, I'll talk about the resolution mate rick that the tgdc asked us to keep up to date. The agenda and aims of the meeting are to-- i'm going to talk a little be it about the focus of this meeting, the strategy of this meeting and then go over the agenda. The first bullet is to remind of an issue I did want to mention. In speaking with the eac, they were concerned that we were referring to this upcoming iteration of the vvsg 2007 for many good reasons. The-- this itter ration by the time it goes through the public reviews will definitely not be adopted by the eac until at least 2008-- I guess 2008, not at least so we have been asked to refer to this as something generic, like the next iteration of the vvsg, or the new vvsg, but not 2007. I would like to quickly go over the research that the subgroups have been doing over the last few months. Hfp has been working very arjew wowsly to update the usability performance benchmarks which are of course very, very important to get benchmarks that are performance based and updates to accessibility requirements, they also have been looking at software independence and accessibility, the relationship between the two. The crt has continued to do research and reliability and benchmarks, quality requirements, electromagnetic compatibility requirements. Sts, of course has been doing a lot of the work on software independence, innovation class research, coordination with-- and paper record usability issues and then more traditional security requirements such as updates to crypt-to, get up access control and system event logging. Now, again, we work very, very closely with the tgdc. Obviously we have had 21 telecoms since the last december meeting. Joint telecoms between the committees, which we think is a very good idea. We don't want them working in a vacuum. We prepared much discussion papers, draft material, and of course numerous individual discussions among ourselves and with tgdc members. We have what we call the draft build this is essentially the draft of the vvsg. It's on the web. Every time we do our research-- and we do drafting, we fill in the sections of the vvsg. We have over 500 pages now. We believe the drafting to be about 80% complete as far as actually putting pen to paper, but that last 20% is going to be very, very challenging, and we're continuing to work with a newer and more usable format for the vvsg. Again,

outreach and support of this research. We have very close coordination with the eac including monthly meetings and countless telephone calls. We clearly are conscious that the vendors play a very important part in this, and they have to imply men the vvsg. We have reached out to them and we do have regular meetings with the via the information technology association of the america there's a subgroup there that's devoted to voting system vendors. We made numerous presentations and conferences and meeting. The standards board is an credibly invaluable resource for us, I believe. I was just there a few weeks ago and meeting with the very important election officials. It has been just invaluable for us to get information about how the process works, and we have had some more formal coordinations with the standards board that ran afoul of facca rules, but we are clearly informally trying to liaison with them as much as possible. Other meetings as well. Outreach to election officials on paper auditing issues starting with the election officials on the tgdc to understand that issue and we have sent some correspondence to-- to get more information on reliability there has been a resolution for nist to create a mate rick and update it to map back our research and our drafting to the actual resolutions, and we are very conscious of that and update that regularly and the website is listed under the third bullet for that. So the aims of this meeting. After this we're going to propose one more meeting probably the end to middle of may so there is one meeting left between now and the delivery to the eac in july. It's very important to us at nist and to the tgdc to reach as much closure as we possibly can at this meeting. It will be very difficult to change the direction in may at the next meeting, so we would like to get all things as much as possible resolved now so nist can be clear direction to develop the vvsg drafts, which of course will be the tgdc product. So our goal at the next meeting in may sensen shally to have a complete draft. So we would like-- as I said closure and i'm going to ask the nist staff as well when they are up there, to make sure they have all questions and issues that they don't have clear direction answered and to please speak up if you need further guidance, so that's the goal of the meeting that I hope you all agree with. The aims of the meeting, again, to make substantial progress on finalizing existing material and discuss remaining open issues and get a consensus. The presentations are broken up in to two days. Day one will be subcommittee presentations, issues and material, and we hope to limit discussion to that material and save some of the cross cutting issues and perhaps more volatile issues to the second day. The second delay be crosscutting issues. The discussion will probably be a lot more ep ended, because not as many decisions have been made, so we need further guidance. Today's presentations will begin with an overview of the draft virginia by john wack, security and transparency committee will talk about the many things its doing, krip toe requirements, access control, software distribution and setup. Core requirements of testing, q&a, and benchmarks for reliability, and then human factors and privacy will be discussing usability requirements, accessibility requirements, privacy requirements, and the usable research update. Tomorrow we' begin with mary saunders giving the presentation on nav lab activities. Although nav lab is clear I will not within the scope of the tgdc, nav lab does activities that relate to the work we're doing, since they have to assess testing labs for competence and testing the vvsg. Certainly we want a dialogue between them and all of us to make sure the requirements we nut there are testable and acceptable to be assessed. The crosscutting discussions will begin with the innovation class, paper roles, vvsg scope and ballot activation, and then there's time for resolutions and future tgdc meeting planning. That's about it. Any questions? Thank you.

I would now like to call john wack up for the next presentation, which is the draft vvsg recommendations, the eaco review. Hopefully I have got the right order.

First I would like to ask commissioner davidson to come back up and do some more introductions.

Our commissioners have arrived, so I would like to take a moment to introduce them. Rose mary rodriguez is filling the vacancy of-- martinez, and carol ine hunter has been selected to replace paul degoie. Please everybody introduce yours to them so they can get to know you, and they will be very interested in meeting everybody. Thank you.

Thank you, and welcome to new commissioners. We look forward to a lot of work together over the next several months. Okay. Good morning. It's always a pleasure to be here and talk with you, and what i'm going to do is actually-- we have a little be it more time-- we're a little be it ahead of schedule, we don't actual I will take a break until 10:30, so I can speak very slowly, which is pretty easy for me to do i'm going to go over essentially, kind of where we are in the schedule, what we have remaining for the next couple of months, what we expect to be doing after the tgdc delivers this to the eac, then i'm going to go through the document itself, and just simply try to point things out a little be it. The document is getting very big, I don't expect all of you have read the thing from cover to cover at this point. Mark twain was a book critic, and he was reviewing somebody else's book and he said once you put it down you can't pick it back up. And that's sort of like the vvsg right now. So with that, I will launch in to this. At the end, i'm going to talk about response to the tgdc resolution 2305, so I'll get in to that. Okay. Simply, I'll just start with what is going to happen right after this meeting. We will make changes undoubtedly, and we still have some general areas we still have to complete, some remaining core material on security and crt. We need help on the innovation class requirements and open-ended vulnerability and some other areas we'll talk about in more detail tomorrow. Final updates to usable that the doctor will get in to later today. Then we have to go through a process of essential I will harmonizing a lot of material. We're highly interested in the document being as usable and readable to the community as possible. We want to give to the eac a document that doesn't saddle them with a lot of reformatting or restructuring. We have got a lot of guide material to write. Thanks like that so we are hoping to more or less be done with the document by the end of may, then we could spend a leisurely-- that's a joke-- leisurely june and july boiling it down to requirements. Right now we have about 920, 930 requirements right now. The final number could actual I will go down a fair amount. There may be better ways to present the requirements than we have done. We will-- well, I guess nist and the tgdc upon delivery to the eac in july will post the draft recommendations on our website, and as before the eac will review this. They may make adjustments. They will put a version out for public review. We expect that we will be involved in vetting with the standards board and other groups, I think the tgdc-- ron and whitney and some others are help two summers ago out in colorado doing the same thing. Final version likely in 2008. Maybe this final bullet right get discussed a little be it. There's pending congressional legislation that may affect things. Okay. With that, let me-- let's see if I can do this with a mouse. Yes. Okay. This is the document right here, and what i'm going to do, and i-- I will try to speak fast, actually, and I'll-- I'll go through it rather quick I will, please feel free to raise your hand and stop me if you have a question. I promise as much as possible to the nist people that I will try not to make up, like, new projects or things we need to do as i'm talking. I do want to say that this document right now, the struck ture of it, kind of reflects the communication we have within our project right now. And that has to be ironed out swhashgs the structure of the document that is. We don't always agree on the material, but I do have to say everybody here on the project at nist really

cares about this material. It's-- it's the first time I have ever been involved in a project where I have seen such dedication from people. People actually really care about the material, and we want to do as good of job as we can. We need clear direction on a number of different items today and tomorrow, and we're looking to you to get as much help as we can. Okay. So I'll start with just a quick overview of the document, and hopefully you can see it there, and it-- you don't get motion sickness if I go through it fairly quickly. Essentially it says six volumes-- really volume six is really just a bib lee august lee ingfy and overview. Frank lloyd wrights grandson designed the front corp. With us, but essentially this is going to be an introduction of the other four come volumes. That will be essentially a guide to the standards themselves. Terminology section is essentially the glossary, and I'll go through it briefly. Maybe I can blow that up a little be it. Scope, applicability. Essentially the big changes here maybe from the 2005 version is we have stuck to only the terms that we're using in the vvsg in the draft vvsg. The final version of this-- these will all be linked. There will be a lot of cross-referencering. These definitions build upon themselves, so we have got that. Volume 3-- volume 3 and volume 4 are actual I will the volumes that have most of the requirements in them, volume 5 has requirements as well, but volume 3 is really the requirements that apply to the equipment, basically. Requirements for vendors. So I'll go through the introduction a little be it. Again, let me blow that up a little be it. Standard things up front. Starting off with a description and rationale of significant changes from reference six, which is the 2005 vvsg. I want to just point out a few things, maybe some people in sts may not realize some other stuff is-- is in this particular area and the core requirements, but we'll go through the conformance clause a little be it. Discussion on marginal marks, those in crt remember a fair amount of discussion there. Actually let me expand that a little be it. Coding conventions, a lot of updates to coding conventions, structured programming, number of things in there. Discussion of cots, how cots is being handled, and I think if i'm not wrong, we'll-- volume 5 as more discussion on cots. Reference models right now we have a couple of different reference models at the very end of the chapter. The section on deletions, what is not going to be standardized, a number of different things, so this-- I think a good introduction written mainly by david flatter, it will be augmented a good be it before we're done. Let me move down here. The conformance clause, and it's not a clause, it's a not a single clause, it's actually a chapter. There's a lot of clauses in it. Basically going over the structure of requirements, what normative, what is informative, implementation statement, I'll talk about the structure of requirements in a minute. Any terminology we're using for classes, now classes, as you know, really are in essence, things used in the requirements to distinguish what the requirements apply to. What-- what sorts of equipment a requirement applies to, classes are arranged higher arkicly. There are pictures right up here this is the voting device class here, and for example, a vv pat is related to dre. Dres can be related to tabulator, and-- you know, basically starting with voting devices at the very top. And when we get to the actual requirements, I will-- let's see-- I will show you a little be it more about that. Semimanics of classes, how they are joined together, very extensions that can be added on. And then I'll get in to the various chapters of the volume. Right now we have got-- is it eight different security chapters that may go down to a smaller number. I'm not-- you know, we haven't figured out the arrangement in general, but let's just say there's security represented in front of you. There are core requirements. Hfp usability, accessibility. There are more requirements written by crt, requirements by voting activity, and some reference models, and I won't go through these in much detail at all. It's my intent to just show you where they are right now. Access control, for example, I believe we'll be discussing some of that, but why don't I just stop here and show you this requirement to give you an idea of the structure. Basically every

requirement has this arrow here. Every requirement now has a title. If you are skimming through the titles, hopefully-- I think by and large they are fairly descriptive of the requirements so it's a shorthand of being able to skim through quickly and find what you are looking for. Green text to make the requirement's body stand out more to people. Here is a class. This applies to the voting system class, which means it ties to all voting systems at this point. Test reference. This points to volume 5, section 5.2. Why don't we go there quickly. Volume 5, section 5.2. Wait a minute-- volume 5, section 5.2. Okay. Chapter 5. Functional testing. So it's basically saying that requirement will be tested via techniques and functional testing. How do I get back to where I was? Okay. So test reference supplies to a discussion field. Many other requirements have it. Where did the requirement originate from? Many are new requirements. Many had their origins in 2005 or the vss 2002 or other standards. The impact field probably won't appear in the final version this is more note to us, but in general is describing what impact this requirement may have on equipment or new technology. Now let me find a subrequirement here. Not a whole lot of sub-requirements in this section here. I think there's a couple down here by pass words, if I can find them. Here we are. User name and password requirement. We have a more high level requirement here. We have two choices. We could then have made this requirement very long and maybe put a table, or we could have put a number of sub requirements, so we chose the sub requirement route here that get in to more detail so a sub requirement has this symbol here, one level of sub requirements basically there aren't sub-sub requirements to sub requirements. That's the requirement infrastructure. I think I'll skip ahead to the crt general requirements. I don't look at those yellow things there. Well, you can look at them. It just means we have material we industrial to fill in, but we noted where it goes. One thing I wanted to point out. Let me see if I can get to voting variations here. You notice these hyper links. David flatter came up with us and it seems like a good idea and it's basically identify the glossary terms used and provide a link back to them back to the glossary. I think tabulator. And it's a way of making sure that these are understood correctly. So couple of other things. So there will be a lot of cross-referencering and linking here, and the idea, again, is to make this as usable as possible. It could be that developers, testers, end up using a paper version of this, to the hyper links at least will identify that it is a glossary term. Crt general requirements. What are they? You can-- you can think of them as the basic core functional requirements for voting systems. Another way of looking at them is that they are everything else after security in hfp, and some requirements in here may actually end up leaving and get covered by some of the other subcommittees, but, you know, just going through some of the requirements here for vote-- voting variations, you can see that what we're covering here crossparty endorsement, so on and so forth. What else are we going through? Hardware. Software performance, general requirements, reliability, accuracy. We'll be talking about these. We'll be talking about electrical workmanship, software engineering practices. For those people in sts, there is a lot of material in here on structured programming, various coding practices, techniques, things that need to be used. A lot of material in here that I would recommend taking a look at. Quality assurance. Quality-- alan goldfind will be discussing some of that. John kelsey will be talking about some of this. When I talk about overlaps this is one example. It could be the audit material may go here. It could all end up in the material section, just as long as it's in one place and you can find it. Our requirements, so on and so forth. Inter operability. Right now we have inter operability requirements they may migrate. These deal with a format for data. Okay. Usability I don't go in to too much, because sharon will do a good job of that. Essentially just in case you don't know already, people think of this as usability and accessibility, but it also has the privacy requirements, and also has new material that I think we

discussed a little be it last time on usability for poll workers, so, again, important material to pick out. Down-- requirements by voting activity, another arrangements of requirements basically necessary to support different activities, so basically election preparation, equipment setup, opening polls, casting, closing, accounting reporting, you know, various requirements on what reports ought to look like. Audit status and readiness reports may be covered here. It might be covered many much more detail perhaps in sts. How the reports are formatted may be required-- may be covered more in hfp. So we have the basic requirement that there shall be reports here. Things about the security, whether they be digitally signed would be in sts ways of representing the data, to the data is readily usable and accurately read, probably be more in hfp. So with that we have reference models at the end of volume 3, which talks about the process model being used in here with various diagrams, and I think we have a uml down below, and this part you will not be able to put down. [laughter]

I'm sorry, I shouldn't say that. It's tough to read this without a computer interpreting it for you. Various vote capture state models, things like that. And any work we do and-- you know, discussion of threats would probably go in this general area as well. Okay. Volume 4 is the other big volume with requirements in it. But these are requirements for vendors and test labs, documentation requirements, and scrolling through this, again-- let me blow that up. Again, it's-- the introductions are well written, and it's good just to breeze through it quickly, and just take a look in general, and does a good job of telling you what is in the general volume as well. Requirements for what the vendor has to deliver to the test lab in technical data package. This, again, is an important area for security. It's an important area for all subcommittees. It's crosscutting, but I think security and crt had a lot of involvement here. Voting equipment, user documentation, this has been a big topic of discussion as well in all three subcommittees. How well it's written. How readable it is. The things it covers. So these are things to look at as well. Per discussions and all telecoms regarding some of this. Certification test plan, test report for the eac, the public information package, we-- dave has looked at the eac's certification plan and material and done his best to harmonize this as well as he can. And then I'll conclude-- i'm doing pretty well on time here-- I'll conclude here with volume 5, and volume 5 here is the testing standard. It does not contain the tests themselves to test specific requirements. It basically contains everything but that. It is in essence kind of introduction to the different types of tests, and has information in the test protocol section, more about how the tests will be conducted in general. There is an informative section, chapter 2, on the conformity assessment process, which is an overview of that, just good to read in general. And then chapter 3 is introduction to test methods. The different types of test methods that will be used here. Vulnerability testing. Another name for that is open-ended vulnerability testing, and that will probably have more material in it. Discussion of inter operability testing, so on and so forth. Some requirements for documentation and design reviews in chapter 4, and discussion a-- a little be it of cots-- cots physical configuration audit. One thing I may have passed over. If you don't mind me jumping back. We had some discussion about what is cots? And the different types of categories we're going to use. So that is in the introduction. I just wanted to point that out, since I think I saw some requirements pertaining to that in chapter 4. And then chapter 5 test protocols. Test protocols-- sometimes these terms are confusing, but the test protocol here is essentially how the test in general is being done, but not the specific test, so how functional test willing be done. Various general guidelines, pass-fail criteria, assertions, missing funnalty, things in here about what vendors have to report on, such as the number of should requirements they-- they meet or don't meet, things of that sort. And in general, you know, that's what we have

there. The bibliography, well, I have got almost half an hour left, I could just go right through and read them all, but--

You are not obligated to maintain . . .

But I won't do that. [laughter]

But we do plan to have an extensive summary. Now right now we have just a summary of requirements table, and we would encourage feedback for the sorts of tables we could put in there that would make this easier to read and ways we could format this better so people can find things. I guess ak are crobat links this already. We can get to the requirements by clicking on the page numbers, but if there are better ways of presenting summaries to the material, and you have advise, we would certainly like to hear it. We're working with the eac as well on this format, we want to give them something they can rather immediately use. So that is kind of it. Are there any questions I can answer quickly on this-- pertaining to the structure, or, you know, the document?

Hi. Whitney. I have a comment and a question. The comment is that I think I was one of the people that sent you down the path of trying to make the document usable by I think nagging is an appropriate word. And I would like to common you on the results. I know this is not an easy task, and I think that the-- layout-- the layout and structure and-- of the document is really-- quite, quite usable and very attractive to read. You open it up and I feel like I can scan through it quite quickly. So a round of applause for all of the people who worked on that and for you for sticking with it. And the question is in volume 3, whether the order and organization of the chapters within that section as presented here is-- determined or is that simply mushing it all together and getting it in to the document?

It was mushing it in together and getting it in to the document, really. It was-- you know, if the tgdc has preferences as to the order, that's fine.

I would love to make a pitch for starting with the usabilitity and accessibility. Of course it's mine so that's an obvious place to start, but I would like to give a reason why, and that is this is a technical standard, an equipment standard, and because we're so focused on the details of the equipment, it's easy to lose track of the fact that the purpose of the standard is to support humans and human activity, so starting with that, and then talking about the technical requirements that support that activity, I think would help us all remember why we're all here.

There-- in the vvsg 2005 was hfp chapter 3, there may be some good reason just to continue that as well. Any other comments that I can get to? None? Okay. Well, I want to reenforce that this is outthere on the public side of the website, anybody can get to it. Anybody can read it. Any vendors, anybody else out there in the community is welcome to read it, and we welcome comments to the tgdc. We post those comments. They are available. The slides, of course, are available as well. Since i'm ahead of schedule, I anticipated that I would go over the response to resolution 2305 after the break, but how about if I do that before the break, and I think I'll still be ahead of the schedule at that point, so that's okay. This was a resolution if my memory serves me right we started discussing in december of 2004. And, you know, coming up-- those-- those of you who worked on vvsg 2005 remember that we had a flurry of activity in december and january to develop resolutions, and the idea, was, you know, basically to put electronic data in to some inter operable format. Hopefully something along the lines of ascii that people can read easelly. And this is the resolution. So

we did some research in to this area. We think it's an extremely important area that-- for a number of reasons, security is where I work and mostly, but in core requirements-- for all sorts of reasons it's important to have some sort of standard format to represent data. Right now oasis eml 1622-- they haven't adopted anything yet, current rev of eml is 4. Dave flatte rsubmitted some issues and a number were incorporated in to the version that's out right now which may be a standard by summer 2007. What we need to do in nist is make sure we get all of the information regarding our requirements for format to both organizations to oasis and ieee to make sure we can at some point reference a standard in the vvsg and that everybody can start using. I any this is-- as we have talked a little be it kind of a chicken and egg situation where we can't wait forever for one standard to emerge because it probably needs some pushing. At the same time we need to wait a little be it longer for both areas to mature fully and for us also to work more closely with them and make sure we communicated our requirements there. So that's what we're doing right now, and in the vvsg we're going to do what we did in vvsg 2005, which is basically have requirements for an inter operable format, and what information goes in to it and in discussion fields, we reference eml. In 2005 we will do the same again in the drafted vvsg recommendations. With that--

Let me check, are there any questions on what john just described in terms of the impact on 2305? Pat?

Yes. Patrick gannon. I would like to provide some additional update to the status information you provided there. The oh say sis election voter services tc did have some interaction with dave flatter, has been requesting closer participation from the staff on that committee to move that forward. The election market language of version 5 has been approved by the committee. It is out for 60-day public review. Once that is completed it will be submitted to krm an oh ace sis stand around the june time frame. There are representatives from the ieee p1622 on the committee. They have reviewed the requirements to find they are a subset of the-- market language standard and that the new version 5 meets all of those requirements under 1622, even though p1622 doesn't have any standard they have adopted to meet their requirements. Right now it seems to meet all of those requirements too, and we are looking forward to setting up some testing-- or demonstrations in middle of this year.

Thank you.

Thank you.

Any other questions or comments for john? Okay. With that, I appreciate him getting us ahead of schedule, i'm sure we're going to lose it later in the day, so with that let's take a 15-minute break right now-- come back-- be realistic 10:20, according to the official atomic clock up there. Thanks.

I would like one of the three of you to come up and present security and transparency progress.

I am glad to get the security and transparency progress report. And kelsey will do a presentation on auditing. And bill will do a presentation on cryptography. So and over you, I reviewed the development process we are using to create credit requirements and then we will go through very briefly and frequently the status of the different security requirements, different topics, grouped by topics. And then we will open it up for discussion. So to give you a perspective on where things are as it is presented in the presentation we first create draft

requirements based on the tdc resolutions. It is [indiscernible] then this full review. We revise this requirements and then distribute that to the security and transparency subcommittee for review. And then we revise the requirements based on those comments. Can we distribute those revised requirements to the tgdc at large for review. These are the ten different cut back areas we are working on currently. He was at the top or a less mature than the ones towards the end of the list there. And you will see that in the presentation. So says the last tgdc meeting we have dealt some draft requirements. Those requirements relate to this bill covers, tamperproof seals, external ports, or covers and panels and casement. Those requirements are being reviewed at this point by staff to be revised and we will shortly be distributed for review. Also said the last tgdc meeting system integrity management requirements have been developed, and they cover areas such as communication, security, malicious code protection, platform configuration management and error conditions and how to alert people to those and handling of those. Those requirements need to be mapped to the previous version to understand the impact, how far we are stretching the requirements and this iteration. In addition, they need to be harmonized with the security and not security the innovation class has come up since the last tgdc meeting as part of a resolution. Initial research and development has been conducted integrating some high level requirements and entry criteria it to the innovation class. We are working with the [indiscernible] to that discern how the type systems could be certified, how to integrate that into their testing and certification program. The group question is how are innovative techniques will be reviewed and tested and a discussion paper was recently distributed to sts for review. And I believe tomorrow we are going to have an extensive discussion on that topic. Security documentation requirements, since the last meeting we have developed a few high level -- very high level requirements. These requirements need to be polished up to map to the previous version. The global requirements -- those are being developed as the different sections or the different areas of security requirements. And once those areas become stable we will pull those out and consolidate them and put them into -- I think volume five is the document? Volume four of the vvsg. In general there are three areas of documentation related to securities. In general security documentation relates to security architecture. The systems are to mitigate some technical documentation provided to how the equipment is designed and implemented to help provide the security features. Those documentations really feed into the testing labs to help them perform testing. User documentation is related to how voting security equipment features are used. In addition, to that it requires the policies and procedures that were envisioned by the factors when this equipment was created. So that if certain policies and procedures are not implemented, other mitigating policies and procedures would have to be in place to mitigate those issues. The distribution of this to sts will probably be more and kind of chunks as a general security requirements -- as the high level security requirements become stable. We will let those out for sts review. And then as the low level requirements become available we will also let those out. Software distribution requirements have been developed since the last meeting. They cover issues such as the creation of separate distribution packets, master copies are sought for distribution packages that have distil signatures on each file contained in that supper distribution package. Requirements relate to the [indiscernible] offered. The types of requirements based upon types of repositories and the services that they provide. Access control requirements, this is kind of a crossover area with access control. That is in relationship to software installation. And we want to limit software insulation to the pre loading not. Requirements need to be mapped to the vvsg 2005 and harmonize once again with the security and not security related requirements. This was recently submitted to the sts subcommittee for review. The next set of requirements relate to

system mapping requirements. These have been developed since the tgdc meeting. The last tgdc meeting, I should say. They cover the types of events that need to be covered such as date, time, type of event that occurred, protection of the log through the use of cryptography and analog management. These requirements have been mapped to the vvsg for impact. Basically that is showing us that the types of events that he to be captured are at a much more detailed level than in the previous version. Also the introduction of use of cryptography into the protection of the log. This was distributed to sts for feedback. It was updated based upon that. One of the comments that we had was to put the events into a tabular form so that it would be easier to read and understand. So we did that. As well as cut out requirements to simplify the requirements and make them less complex. One of the big questions that came up was how configure how should the system of analog and capabilities be? And general-purpose operating systems, the configurability of the event log is built in pretty much into the systems. However, limited use operating systems such as in the process, single user operating systems are a better operating systems probably don't have the capabilities. And so we are working with sts to scoping requirements appropriately. And once that something is done we will redistribute it to the sts. Access control requirements have been updated since the december meeting. They cover things such as the authentication mechanisms, access control mechanisms, management of the identities and rights and limitations of rights during the given most of the system. They have been mapped to the vvsg for impact analysis. And one of the things here is that in the previous version authentication mechanisms really focused on the use of passwords and those types of things and very detailed requirements related to passwords. So what we tried to do was to open it up and give them better requirements in terms of the use of hard work tokens for authentication. We reviewed the impact of stuff for independence on this. Originally these requirements were developed before the passage of the software independence resolution at the last meeting. And it turns out that software independence really did not have an impact on that come on those requirements. We distributed the requirements to sts. We updated it based upon their feedback, and once again there was a requirement on how or why should the access control policy be? How flexible should this be? General-purpose operating systems have these available. It is the limited -- limited operating systems that don't. We are working with sts to stop these requirements properly. Once those our scope we will redistribute those to sts for review. We set up validation requirements that have been updated since the last meeting. They deal with supper identification and verification, inspection of registered variables and registers and variables and other equipment property such as the levels of power that is left in backup power supplies. Being able to determine if the communication capabilities of the system or -- are on or off. Does the equipment have correct level of consumables in it such as paper and ink? They have been mapped to [indiscernible] to those five. A lot of the 2005 was [indiscernible] and verification as well as having the variable resistor inspection. So a lot of the new requirements in this section relates to the other properties, in a sense. We want to expand the scope away from just the software and the registers. So again, these requirements were developed before the passage of the software independence resolution. So we went back and looked at what areas that suffer - - software indepedence actually impacted these requirements. Was software identification and software verification requirements. The ratification requirements did not really have too much of an impact on it. However on the software verification requirements it did have some impact. One of those was that it seems excess -- acceptable to allow internal verification of installed software for non network closed caption devices. Not that work is kind of a misnomer here in the sense that it can be limited -- limited network should be the actual -- is more descriptive of what it is. What we mean by limited network capability is that a low capture device could

communicate with one election management system or one other low captured device. So very limited communication with other devices. What does this mean? It means that an external interface to check the installed software is not required on those limited network type of low capture devices. I guess the concern -- so -- okay. So then the external verification is required for election management systems and network vote captured devices, fully vote network devices. And the reason here is that the election and systems and network vote capture devices to communicate with several different devices during the process of the election. And in that case there is more chance of getting -- of systems getting infected with viruses and stuff. It seems somewhat appropriate to have election management systems have this because in most cases those systems are on general-purpose pcs that already have external interest on them. So that was the justification for that. These requirements have been distributed for review. They have been updated based upon the feedback received. Some of the feedback received was to reduce the complexity and possibly try to raise the level of the requirements higher. So we discussed that a little bit, and what it means is, if you had different types of verification techniques, some that are cryptographic and some that are not you believe that level of granular. So what was discussed is, should the vvsg support other means of -- and cryptography for verification techniques. And it was decided that in this direction because they are non cryptographic based techniques are at a very intimate stage in their development that this iteration will be explicitly call out cryptographic based techniques. Those updates will be to be redistributed to sts for review. Auditing requirements focused [indiscernible]. The capabilities of the equipment to support auditing, requirements based on electronic and paper records. And that was recently distributed to sts for feedback. Kelsey will give you more detailed presentation on that topic. And cryptography requirements, the requirement has been significantly updated since the last meeting. Eliminate the tutorial style that it used to have caught the tutorial of that section. It still focuses on using the [indiscernible] and really focuses on the management requirements and trying to get -- to make team management a workable solution and simplified. It was recently distributed to sts for feedback and you will receive a presentation that more detail on that topic. So that is what I had.

Any questions? First I would like to acknowledge our presenter. Any questions?

Thank you, Dr. Jeffrey. As you probably realize this is always tight a -- quite a test for those of us that don't do this type of work on a regular basis, and you speak a different language that we do in the election community. And therefore I would ask if you could put this in maybe a succinct description of exactly what you are trying to accomplish when you talk about your set of validation and some cryptographic changes and granular. As I think I don't deal with on a daily basis and would like to know what it means and what the implication is for the equipment and for the election officials who will use the equipment.

You want me to go ahead and take that one? So what we are trying -- my understanding of what we are trying to do with a set up validation is to provide the capabilities on the system that allow election the officials to inspect properties of the system so that it is to about so that it is -- so that they can be confident that it is ready for use at the polling place.

Are these directions that you intend to be given by the vendors to the election officials or are these standards that you are attempting to define that will be distributed universally, kind of a universal design for how set up will be validated?

The goal is to provide the capability in the system, and it is up to the to restrictions to decide whether they will use this capability is to validate the system. The different areas of the system.

What I guess I am trying to understand is -- I see what you are attempting to do. But are you saying that this is the singular method in which the local officials can validate the set up? Is the only method they can use or is that something to -- the management guidelines of the ac or is that subject to state law? Are we setting up here a validation that the that is a simpler method that everybody must follow or else it will not meet the guidelines?

I hesitate to say that their methods, as much as the capabilities of the system that are available for use if election officials wish to have them.

Would you like to add to that?

Maybe I can comment to help understand a little bit about what the set of validation is trying to achieve. It is requiring the machines to have the capability so that officials can, if they choose to, to inspect the machines to check some of the things that you might care about if you wanted to check to make sure they are ready for use. For instance that includes things like taking the supply consumables. Is there enough ink? Was it configured as you thought it should be? You can check what software is currently resident on the machine. It allows you to check and confirm, is that the certified version of the software that ought to be in there that has not been tampered with or replaced. So the set up validation requirements in the standard would require vendors to advise this capabilities. Some of these have appeared in the 2005. It is worth pointing out if the security part of it that allows you to check what so far is residents -- nelson advised this would be a partial relaxation. So compared to the 2005 to 13, that required as I understand it all machines to have the ability. And this would be a step back from that to say a subset of machines required to have that specific ability to check what software is resident. I don't know if that helps.

Well, that is helpful and that me ask one other question. Are we talking about the initial set up of new equipment upon delivery are we talking about the set up each time the equipment will be used for an election?

My understanding is that this is that you would envision could be used before every election. For instance, checking before every election if there is a sufficient supply of ink. That is something he might want to do. Vendors provide that ability so you can use it if you decide a search.

One of the things I think that might help you understand that is a lot of times software -- do software is installed on existing hardware. And a lot of times election officials are not sure it has been installed on every piece. That is within that precinct or within that county. Has been found before the supper has been installed but was not installed and all of them and that caused problems on election day. So this gives you a way to verify what software you have in the equipment. Does that help?

Well, that does help, commissioner, but I guess I am still struggling with the thought of whether these are for the purpose of new equipment that is being set up for use it to insure that all these different configurations are present as opposed to what you just suggested which is existing equipment that maybe was not certified under the new 2005 guidelines that is going to have new software installed. It sounds like you are talking about equipment that is under ongoing

use of upgrade and update. So these set of delegations would apply to that as well.

Now, what we are talking about -- with the standards we are talking about developing now it is the future. How it is working right now obviously is going to continue working with the vvsg 2005 or if you are certified to 2002. What we are doing here is talking about the future. It may be four years out before your equipment will be able to tell you if you have software that is updated. I don't know what the timeframe will be right now because as we said it probably will not be adopted until 08, and then we have got to have the meetings with the manufacturers and everybody to see how long it will be before you can develop this. And how long will it be before we can expect it to be purchased by jurisdictions? So we are talking about the future. It is not changing the past. This is the future.

I guess you would be the right one to answer my question. One of my concerns is that we maintain a broad line or a fine line between election administration and elections management guidelines. So there are a lot of ongoing set up requirements that are going to be election management issues, not equipment issues. So if I am clear about these set of validation as we are talking about precisely the equipment to ensure that it has what it is promised to have.

Correct.

Post certification and test or post testing and certification.

Maybe I can have a clarification.

It like it ask people to give their names of the record, will be easier.

I do the set up the allegations as the updating of the zero tapes situation. But the zero take you are checking that certain [indiscernible]. But with this there is more moving parts to them and you want to make sure that those are and the proper state as well. So sometimes you can do it as the capability of putting out is to rotate, but it is just checking many more things.

Are there any other questions? Okay. Thank you. Next is the discussion on cryptography requirements.

Good morning. I am bill burke, and I get to do the exciting part I guess of trying to make the incomprehensible comprehensible, something like that. When you do a talk like this the sad fact is that you are either talking over or under somebody all the time. And I don't want to talk or I say, this is all magic. I am a wizard. Trust me. And by the same token for all of us at some level of cryptography we cease to be wizards and we have to rely on somebody whose expertise is deeper or better than our own because various things become very specialized and there are only a few people often in the world you really seem to understand certain things. In any event what I am going to talk about here is the cryptography section as it stands now in this current draft. I am going to walk through questions. It is going to be a fairly high level walk through. I actually have more detail and the slides will try to address specifically. But I will point out what I think are the major implications. And in this particular draft of the document, as nelson noted, we have taken a tutorial that was in earlier versions out. I guess largely because in the standard of this sort or as required by required by requirement it is hard to see how to fit a tutorial in. And in any event the straightforward way to specify this is to write the specifications for people who knowledgeable in the

art and that is what I have tried to do. So I will try to explain here the logic behind what I am doing. I don't expect election officials to read the chryptography section and get a tremendous amount out of it directly. I expect people to implement cryptographic stuff to read it and understand what i'm talking about. The first part of the cryptography section just sets some basic ground rules. The first and most fundamental one is that all the cryptography will be done in a validated cryptographic model. 140 is a federal implementation standard that outlines the scheme for testing cryptographic models. And it includes a list of approved models or improved algorithms, and the have a bunch of labs that are actually quite practiced at doing this. And so it seems an obvious thing to do to take your cryptography and plug it into the existing federal systems. I will also say these labs now exist all over the world. We have been in germany and england and canada and the united states. So the first thing is that cryptography can be pretty rigorously tested. As far as the mechanical level. Then you know at least that you have a good sound cryptographic piece. It is never the least bit difficult to take a good sound cryptography and use it in a way that is totally insecure, but that is at least a start. The other general requirement is we specify the minimum of what we call 112 bit cryptography. And all that really means is the generation of cryptography that we are requiring for federal use which we think will be good for at least another 20 years or so. Beyond that it is actually very hard to make long-term projections. Things like quantum computers cause almost a change in what is secure and what is not. So we have stronger stuff we could give you. It might be secured longer than that even, but that does not seem to have much of a point to it. So that is a list of the algorithms up there. I am not going to walk through them. You could use the stronger stuff if you wanted to. It would not bother us. I am going to far here. So what is a group of module? That would be worth talking about specifically. It is basically a separate distinct program or a device, a piece of hardware in which you to just basically cryptography. We have mentioned a test program, and the big distinction I want to make here is roughly speaking you can break modules into two kinds of things, suffer modules and hardware modules. Hardware module is its own dedicated the piece of hardware in which you do nothing but cryptography. And typically it is a little microcomputer. Basically inherently not very different than any other microcomputer, a $2 part basically in many cases. What we are doing here is fairly conventional which is to say most of the cryptography that you do in the voting system you can do in software as a part of the general software system that you are running. However, we are identifying this particular digital signature functions that are what actually protect all the information and it is having to be done in a dedicated hardware module. And the reason for that is basically because it gives you an extra measure of protection against problems in the overall software system and the possibility that there is malicious code in the overall voting system. It isolates that in a separate little fairly well protected sandbox. So I wanted to give -- yes?

Let me just clarify what I think I heard. One aspect of it. We are specifying certain cryptographic algorithms and we expect overtime your estimate currently is like 2010 or something, but it could be sooner or later when one might have to upgrade algorithms?

No. Well, the 2010 date is the date by which we are trying to kill the old generation of stuff that we had in the federal government since the 1990's.

Understood.

And that is not even included here. There is no point in introducing here a standard that won't even come to use until 2010. Cryptography we would like to cut off.

But we are looking at something which can change over time? Are we introducing the idea that the guidelines will be that these systems should be designed such that there modulars are enough that at different points of times you will be able to swap the algorithms?

Well, certainly that is mostly easy to do with software modules. This is something we should get clear. The notion of the hardware module is that certain segments of functions are built into the hardware and they don't get changed at all during the life of the machine. At some point you would have to have a new voting machine to replace that, and I am saying, we think we got at least 20 years of good security and cryptography. And the thing that really puts the damper on all of this is the possibility of quantum computers which fundamentally affects the security of all the public key algorithms we use today. And that is why I want go any more than 20 years.

So you are not requiring the ability to upgrade. You are just saying that --

I am saying that at some point in another 20 years this is the computer world and I realize that election machines have traditionally been used for very long periods of time. But I cannot project security well enough to want to specify anything beyond about a 20-year period of time or tell you it is good. So I want to speak a little bit on public key cryptography.

I am not sure -- david wagner. I'm not sure if you got an answer to your question. I don't know if we have discussed this among sts. My feeling is, no, it should not be necessary to require the ability to do field upgrades on your crypto algorithms for voting machines. Crypto, as bill explained, is well enough understood that the crypto algorithms put in place ought to last for the lifetime.

Right.

But the only thing that really -- this requires that puts a limitation on that is the signature part of the hardware module because it will be easy enough to replace him anything that is done in software [indiscernible] what people will choose to do because the truth is the processor is likely to be more powerful than the one in the signature module itself. And because basically what we are requiring the hardware module to do is very specialized. So there are a lot of things that could be upgraded. I don't see any real need that they should be any time soon. So now public key cryptography, this is something that is actually pretty recent. It did not exist 30 years ago. I think by not just about everybody has heard of it. It goes with the awful initials pki that kind of terrify people. And the concept is really pretty simple. You have [indiscernible] related keys. There is a public key that you can make public and it is usually presented as a thing called the public key certificate. And you can use this public key to either encrypt data or to verify a signature. And then associated with it you have a private key which must be kept a secret. And with that private key you can either decrypt in cryptic data or you can use it to sign a digital signature. And it is the digital signature operation that is the key operation for what we want to do here. If you think about it, for most election systems there won't be a lot that you will be encrypted. Possibly if you send results electronically back to an accounting center or whatever you will want to encrypt them while they are traveling over a network or something

like that. And in some kinds of schemes that we might get into and when we go beyond the innovation class systems they will probably be more uses for encryption. But the big thing here that we really want to use cryptography for is to protect and authenticate records in use to -- terms of parenting the authenticity. I have already talked about is the signatures at this point. What we do the digital signature basically is first to generate some think of the hash or whenever it is we are going to sign. A relativelwhy short compressed representation of it, typically in the next generation of stuff we are introducing here. 256 bit digest of the message. Then we apply the private key to it, and we get out the signature. So if you want to think about what actually goes on in the voting machine typically the tall software of the voting machine probably does this hash. And then it passes hash to the little hardware model that I have already mentioned to actually perform the signature operation that is basically what is going on. With signature verification lever is verifying the signature takes a look at the message and generates the same hash of the text of the message and then applies the public key to the signature field message. And at least in the simplest game compares the hash that it then gets as a result to the hash that is on the message. And if the two are the same the message verify. The verifier then knows that he has an authentic message if he has the right public key, and not a single bit of that message has been altered in any way since it was signed. So this authenticates the message. The practical applications of it is -- are, I should say, that is largely eliminates chain of custody issues. You have a good sign message. You really should not care how you got it. Whether it was sent by passenger pigeon or just given to you or you found it on the street. If you can verify the signature he had a really strong check that it is an authentic message and that it has not been altered. The point is, until you apply a digital signature or some other cryptographic techniques to data there is nothing in the world more alterable, forgeable, changeable than data. But want to put a good electronic signature on it and a signature scheme you have really liked it down in a way that is actually stronger than you would typically get with paper because the paper you are looking at a document and have it was cared for. And then if you are worried about simply altering it you looking at very detailed forensic evidence to see if you can find evidence. Or evidence that the paper is forced somehow and that the whole thing is a fabrication. But it is the signature you really lock things out in a good solid, very easily verified format. So we are interested in this because we want to produce electronic records, particularly audit records that we can sign and be pretty darn sure that they have not been messed with, fabricated, forged, altered, changed in any way since they were signed. I turned off my microphone and of it to advance my slide.

Hold on a second please.

Just so I can catch up with the then, what you are talking about here is really ought to a post-election function, the transmission of information by some method that is to be encrypted to insure its integrity while it is being transmitted. So we are not talking about a function during the election.

I am talking about signing the data as you create the audit records during the election and then when you examined those audit records you can verify the signatures and verify the authenticity of that data.

And we are primarily talking about the equipment?

Yes.

That has a to still --

If you look at what -- and what will follow in the next stop, what we are interested in being able to do more than anything is with dre equipment and the human verifiable paper audit trails we want to be able to rigorously cross check them. And we want to be sure that the electronic records -- the electronic audit records that we are cross checking have not been filled with some how.

Well, I am going to ask a lot of probably what sound like kindergarten questions, but I have to ask them on behalf of election officials who don't understand this any better than I do and I had been reading the minutes and resolutions and material prodigiously. Some of these things are so confusing. What we are talking about is the outcome, I guess, the results that you want to audit. We have the voter verifiable question as one form of auditing, but that is not what we are talking about, where the voter it to verify what the voter casts. You are talking about a different form of authenticating the outcome. Is that correct?

What I am talking about is using the cryptography to create electronic records that can be fully or complete authenticated so that in a major audit stage where you are actually comparing, typically, the paper to the electronic and making sure that they are consistent, then that you can be sure that the electronic part of it is authentic.

Let me just finish my question. We are talking about a triad here in. Voter verification on one hand in the course of the election cycle. Errors arise. Hopefully a voter checking their ballot representation by sea and air. Then you also have the paper trail so that you have another form of terrifying a digital will cast that can be used for recount for example or audits. And what you are talking about is, I think, a third thing which is to make this the source or the security of the distilled [indiscernible] safe and so secure that it is beyond question but, beyond debate as securing the signatures, I guess you call them with integrity for recount or for some other purpose.

But what you want to know is what machine it came from and that's as it was produced by that machine it has not been altered at all. And what we are actually worried about being able to reliably catch more than anything is the possibility of malicious code in the voting machine. Printing one thing on the paper and putting something out electronically. And we are just over all trying to come up with a system. This is really his talk and not mine. And he will go into this in some of gory detail.

You are our present witness.

I am the present witness. The present witnesses not as well prepared.

Feel free to have john comes up next to you to help answer the questions.

Could I comment?

Certainly.

Maybe I can relate to something that we currently do procedurally. When you close the polls on many of voting machines typically there is some memory card for removal storage media where the votes are stored electronically on that memory card and then it is rate, and in many places that that memory card is transported by poll workers back to county headquarters and many places have a chain of custody requirement. There has to be two people accompanying that

memory card or other requirements to make sure that is not tampered with by the transit. This one of the things a party can do to you is project that they using mathematics and a way that prevents temper and with the date on that memory card while it is in transit. After you have closed the polls so what that does is it reduces or maybe even eliminates the requirement for this two person control on the memory card. It eliminates the opportunity for swapping of memory cards either or modifying the data on the memory card while in transit. This is a different issue from the voter verification. This does not ensure that the vote was recorded initially as the government ended. It just means that while it is in transit is not going to be tampered with.

That is why I ask the question about the transmission issue. This is a transmission issue.

It is some other tabulating are county center. Is this what then we talked about in terms of hardwiring each machine? This is so it has a very specific encryption and can only be used for that particular precinct? It does not have the ability? Is that what you are talking about?

I am not trying to do that. We are definitely not trying to do that. We are trying to ensure that you can always tell which machine actually generated these records. Okay. But we are not trying to actually, in the cryptography section for sure, specify anything about whether one machine is producing records that are somehow tied to a particular polling place or not. That is kind of beyond the purview of a cryptography model. And I suppose people might want to choose to set things up that way, but it is not the intent of this document to pin you down like that at all.

Well, thank you. I don't have any other questions on this and it is very helpful to me. I appreciate your explanation.

Another are some questions about fingerprints, but it is interesting that each machine has a unique entity that can be known. So if I decided that machine one is in precinct 25 and there are results back and say it is from precinct 26. I know that -- I know that those -- let me back up. I know the results I got came from that machine and not from some other source.

You know what machine it came from. If you thought the machine was in prison -- in the ballot on it says it is 26, somehow you have gotten an inconsistency in your record somewhere and you ought to be looking into something. But this is below the level of the card for -- above the level of the cryptographer.

But again, you are providing a capability that can be used as part of the election process better than requiring that.

That is the idea. I have already talked about the signature model which is a separate chip, a separate microcomputer. A $2 part once you get it in volume, but of course there will be some serious development costs associated with making sure you have it right in the first place. One of the things that we have chosen to do in [indiscernible] this is to require that it generate its own key because we want to try and make the operation of this thing as seamless and transparent as possible. And also because having it do that actually eliminates a number of ways that people could it have to fiddle with the system and manipulate the keys. So the private keys that are used in the siding operations call the idea is to design the model so that the key is generated at the private part of the module and it never leaves the module. This is one of the ways that

we help to prevent the effects of malicious overall system code or code that has been compromised from tampering with the results successful appeared.

We have some pieces of software that require me to plug something into my machine and the software won't run unless I can prove I have the one and only a little hard work any that up again. That is probably not exactly the same, but is that the sort of thing we are talking about?

What I mean in this particular case is that this is not something the plug on to the machine. Is something that is actually personally soldered into the machine. So you can think of it below -- or when we reached a high enough level of the integration in these parts it might just be a separate little piece of the actual chip that does everything. It is a physically distinct device that is probably in most cases a separate --

Bill, I think the answer is yes.

Okay. Fair enough. The answer is yes.

This is just a list of the capabilities of the signature module. It has to generate the key that implies some stuff about requiring a random number generator on the device. But it has to be able to -- there is a public key center of it that identifies the public key and it has to be able to store and output that and to create those. And everything else really can be done that you wanted to cryptographically. There is a surprising amount of cryptography that goes on any computer system whether you know it or not. You can just be done in general software on the voting machine.

Just for application, and generally speaking it is good practice to have the signature module be in hardware that can not be accessed by anyone else because what is fundamental is that property that he is talking about cannot be done by anybody or accessible by anybody because that is what is taking these elements of the record and binding it and signing it so that in that transit you cannot change it. So you want to make sure that nobody can have it in software where they can access that keep or make that. That way I could tamper with it. I could modify the key and resign it. But if it is embedded in that machine into space out and you cannot access and find out hen you achieve the objective. So for most applications we always insist that the private key be in hardware and not accessible by anyone.

Secretary of state in nebraska. This is bit of my concern and maybe it is not testify, but in virtually every election there is a lot of ability of the equipment between precinct. One precinct double in size over the course of the summer and the companies to be assigned to that precinct. I just want to be sure that we are not encouraging machines in such a way where they can only be used in a particular precinct and don't have the ability that we are used to having.

It I could respond. That is an interesting concerned, but not one that is a problem here. The goal here is to give every machine its own identity. So you know what it comes from that machine. The rules, possesses the present and what those machines to, whether they are acting as tabulators or vote captured devices, all of that is that a higher level of management. There is absolutely no intent here that we are getting rid of any of that flexibility.

Thank you. That is very helpful.

Basically there are two kinds of keys. There is a long term device signature key that basically we are requiring it comes with the device from the factory and last the life of the device. Then there is a short term signature key that you create for each separate election as a part of the start of process for the election period is used to sign the records for a single election. And then when you close the machine out at the end of the election the key is destroyed. So it does not exist any more and cannot be used by somebody even if you get possession of the machine to later fabricate another version of the records. So that is the scheme. It is intended that if somebody does a good job of implementing it, it is almost transparent that this is going on. You have to set machines up for elections and help. And it should be an automatic process to generate the keys. You have to close machines at the end of elections. And the destruction of the keys should be an automatic process. The necessary records should be automatically created as a part of these things. So the actual people doing this should hardly even be aware that this is going on. That is the intention. The device signature key, which is the permanent key, the one of the requirement is that it include in the certificate that goes with the manufacturer model and serial no., at least whatever the actual and part of the machine is. And that same nomenclature should appear on the outside of the device. So then it is relatively easy to match the two up. So you have the electronic version of the certificate that tells what the public key is and you should be able, by just looking at the outside of the machine, to know which voting machine that applies to. That is the intention. The elections, as I said, is generated per election. And one important point is that you keep count to the number of keys that you generate and the number of times that each product is used. And as a part of the auditing process you should be able to account for every to tell you create and every time you sign something. You ought to be able to have -- to produce the record that was signed when you did that. When you close the election out you produce a signed up but that tells how many times the key was used and the key gets erased. So the idea is, be able to account for all the audit records and then give you automatically in this little hardware module everything that you need to do to do that. So the basic summary of this is, we are calling for a hardware module will to do signatures that at some extra cost to the voting machine as opposed to doing it in software. It gives us extra protection against software that has been tampered with. There is a permanent key that is associated with the device. There is new key for each election and we have tried to do everything so that it adds that the management of the keys has very little extra to the overhead that is already involved in running the machines and close them out. And that is basically the whole talk.

Thank you for crypto 101. Are there any additional comments or questions. It is obviously very detailed, but it is an important section. Certainly not something in your normal vernacular that people deal with. Are there any comments or questions?

Thank you.

Okay. I will be doing the opposite of what bill was doing. He was talking to you about something that most of you are experts in and I am not. I will be talking to you about something that I am not an expert and and you guys are. It will be like this in teaching the class. So I want to be clear up front. What we are talking about here is [indiscernible] that address known attacks, not threats. We know that there are threats to voting system that can only be addressed procedurally. That is pretty obvious and everyone knows that. We have this nice requirement for spot for independence from the previous tgdc meeting. So for independence means that the voting system -- and attack in tampering with the software and the voting machine can be detected. It is possible to see that

there is an attack going on or an attack happened. What we want to do here is talking of what is required? What procedures must supported so that it will be detected with a high probability? So basically this amounts to requirements on the equipment and requirements on what the comment does on the documentation and how the equipment is tested. And at high level all this will apply to the innovation class and we don't know much about that will look like that. Okay. Talk about the threats we are addressing. Really all we are talking about here is -- most of what we are talking about is does that involve tampering with the software of the voting machine. You want to say, given that we have these voting machines that have paper records that the voters can verify, what could happen? What could happen if some be tempered with the software? And then what are the defenses to make sure that would be detected? Like I said, we want to be sure those attacks -- those defenses can be used by the election officials given what the contest. Let me help forward. At a high level we are really doing two different kinds of attacks we are worried about that involve tampering of this offer. One kind messed up the damage between records that we have. So for example, if the voting machine just silently changes about. You think you voted for [indiscernible] a recorded vote for jobs electronically there will be a discrepancy in the wreckage. But the type machines will say one thing at the papers also something else. You check those records against each other you will catch that. The other kind of attack and the presentation of [indiscernible]. And the machine be headed. So for example, if the machine introduce errors that are kind of favoring one candidate over the upper or if the machine in the case of operational test and sometimes just prince -- tells you you are voting for knarr and printed book for jobs and record to the chocolate those our banks want to be sure we can check. So there are two different glasses of auditing steps that are supported. Okay. Let me just skip ahead to the diagram here because it is a lot nicer. This is picture and put in to try to explain some of what we are doing it. I think I have a pointer, yes I did. These three areas are sets of records produced by the voting system. And I am not sure this is exactly the right way to refer to this, but the idea is there is this process were voters check in and there is something entered in the poll. Normally it is a manual process. This is so you can verify the number of ballots cast is not way higher than the number of voters again. That would be an obvious problem. And each ballot, you know how many of them were given out and how many were received. You have a requirement for this check that is an audit. We normally talk about this with paper records where you are just looking at the vote for verifiable paper records and looking at the electronic records that are kind of the summary for the outcome of the election for that machine or that precinct or whatever and checking them and making sure they are the same. And recheck your to make sure that the electronic summary of the votes wound up correct in the final election. It is part of the verification process. You can see this picture. All these are steps that are being done. The want to make sure that all of the voting equipment provides all the information necessary in these reports to make this as seamless as possible and that we get the advantages of security in particular by from here to [indiscernible]. These are all kind of apple pie requirements and there is nothing very controversial and these first three. But to really want to do is make sure that the voting system provides enough information that we can catch it if, for example, the voting machine -- say you have a voting machine. If it were to wait until quiet time when nobody was around and then the electronic record and print out three or four extra votes you want to make sure that got caught. You does want to make sure that the difference summary records or the different records from the system give you enough information that you would reliably catch that or that you could if you did these auditing steps. The picture here is, you know, you just want to make sure that ideally in the election report that comes out of the italian process gives to the breakdown by polling place about many of the kind of bells there were. And you can check that

in a fairly straightforward way. If there is other information that is to be included to make this work out I would like to get some feedback on that. The other thing is that we want to make sure it is possible to take these electronic summary records and make sure all the same information is included. So, for example, all this affirmation about how many votes and each type has to be included from the paper records at but the chart records and the final report so that you can make sure they are all in agreement. I was surprised -- and, yes, I report. There actually were some pretty surprising problems as far as not having all the information necessary on the paper records. We want to make sure it is required that every -- if you have a paper roll, the newspaper will have to have the machine -- the entity of the machine on it, which election invalid styles are used in all the stuff. And then you have to deal with marking the write in because those must be handled differently. The final election report into [indiscernible]. It might be possible for the process to provide you with a breakdown of five voting machines or by pulling our present depending upon how you do that. [indiscernible] you want a set of paper records at a time the you can count. You don't want to require people to hand recount everything from the entire polling place. Pretty straightforward. The last it -- bit is where we get into some of the [indiscernible]. The idea is you want to be able to reconcile the total from each machine. And all the information that you need to verify it was done correctly. The idea here is, these electronic summaries are ditigally sign and the indicsernible side in a way where it is bound to a specific election. Once these are produced it is committed to buy the machine. If you took the machine apart and to the key out you could not go back and produce it and back to your records. It is kind of nice feature to this. We have these electronic summaries of the voting records digitally signed and we have this file election port. Every wanted to we can actually put these out and post these on the web worshiping and ready could check that this summary was actually included in here. Each summary for each machine was included in the final report. There are some to privacy issues you must do with billing ballot right and because those won't have been resolved it. We are at the point where the machine commenced to how to solve the problems and are included on the record. Must deal with that and there are ways of combat or you could agree goes into a different [indiscernible]. The thing here is that this park right here, I believe [indiscernible]. You could look at this electronic summary. You can print it out and verify it is concluded correctly and you could verify the signatures here and here and it is kind of nice. It adds verification that nothing has happened in between the time that was committed to. Okay. So in summary, I don't think anything here is very difficult or surprising. I think mostly with just want to make sure it is written down and required. So all the data needed for these accounting steps that we know address specific attacks must be included. We want the electronic record to be designed because that that security at essentially no cost. You are using the existing tool. These requirements will have basically no impact or very little impact on the cost of operating the voting equipment other than what is required to get the crypto module in there. Everything else is just to change a little bit of software to make sure he can generate all the right report. Are there any comments or questions on this part?

This is paul miller and I have a question. You made the comment about unambiguously being able to ratify the paper tape as part of the cd pat. In terms of my analysis of my understanding comes from broken paper tapes that they did not the second half of the tape put together with the first half and that they switch printer modules from one machine to another machine. Are we contemplating some kind of a requirement that the machine be able to sense when a new paper will has been inserted and print the indentifying information at that point in time?

Yes. I know we have talked about that -- there are places where this touches on reliability requirements that I think we have dealt with as far as not having the paper tear easily and be able to change the paper will not causing problems. But in the paper records requirements we have been working on one of the requirements we know has to be there is it you change paper rolls the machine has to know that you changed the paper rolls and be able to prevent fires.

Dealing with the special take to the cases, the police -- that needs working out. But I think those are all really important issues because that is a place you would get breaks.

Thank you.

Where in the tvsg is all this auditing commission requirements?

I believe -- this was talked about. There was some question where it was up in the securities section with the other section cannot forget where it is in the current outline. There is an entry for it although it is not filled in yet because it is still in the process of being edited. And it is actually a big concern. This is where we need input from elected officials because they have done these audits and will be able to point out think we are missing.

I have a follow-up question. For electronic records how is that being addressed? So far the only thing we have right now is interoperability and some high level requirements.

Well, the electronic records, we have a chapter on electronic records that has been sent out to the sts that has not been put out here and is still being worked on. One of the requirements we have there is that electronic records have to be produced in a complete the specified format so that you can -- if you need to you can write your own shop for and don't have to depend on the vendor's software to get information. There is some thought about using the ml centers. There are some issues with that and I think that dave can address the. There is a lot of the still there.

Secretary of state, nebraska. One question that gets me adjusted little bit is this seems to be in the area of election administration and does not seem to be standards or guidelines for voting equipment. We are starting to get into the area of how election officials and pull -- poll workers or cord to perform the job. It seems like tgdc is starting to draft someone into the other half of the election conduct. Half of which is your equipment and the other half is an illustration. And in looking at your chart are looking at some of the procedures you are suggesting, it also is to be far beyond the equipment. They have to do with the conduct of the election administration% to be purely an election assistance commission issue and not a tgdc issue.

David wagner. I think that is a very fair concern. I don't see that as an issue here. Sts has asked us to look at and understand what be auditing procedures on the typically used by election officials around the country and to develop requirements to insure the cord can support those -- have election officials are using the [indiscernible]. So this is not by any means mended the procedures election officials will use or how election officials have to do the audit. Whether it is ensuring machines provide the information election officials will need to bill to do those odds and to make it easier to do those odds. But whether those audits are done and how they are done is entirely up to the official and not something that the standard board regulates or require.

How would you include this in a tgdc report to the usg it is not a standard that can be tested to or certified to. It is up to state law.

Deadline again. This survey of the other -- of our procedures is the background that will inform the drafting of requirements for equipment specification. But those are the specifications maps they are things like what the machine id might not be printed on any of the records.

That was informed by the research service of our procedures which came out of the server where it was discovered election officials are having a hard time using these records to do audits because they did not have the machine at the far printed. So that is a requirement we can make on the call but that is testable and can't support the election officials needs.

That makes sense to me in terms of helping to ensure that the equipment provides information to do audits but also to go ahead and say, these are the kind of august you should do. It seems like we are beyond the quebec.

This is bill jeffrey. This will not include procedural issues that are done at the state and local home. As david said, it would only ensure that however you do it, hopefully there is somewhere we have captured all the data necessary. You have all the information reliably with the files integrity. So in reality the entire to our requirements will encompass things that members of the to do that nebraska may not use. We may use a subset of it. [indiscernible] may use a separate subset. But we are describing is try to get the idea of how any of it was thought so that the relevant data is captured by the will tell you how the state of nebraska would never do an audit.

And that was my concern because the you see will be coming out of the election that I got my sometime later this year may about the same time the sets. And the two things must be compatible given the sets, standards or guidelines for how to conduct a recent audit of. I think this will be able to answer the requirements on the hardware and not procedures. Whatever procedures are generated will hopefully have all the data they need and what we are trying to do is capture to make sure that anything you could possibly want in your audits is put into the requirements in such a way that is secured and the integrity is short.

Thank you.

If I could [indiscernible]. If I may, mr. Secretary, having just gone through a hand on it in the last chart election it would be impossible to do that if the equipment did not give you, as they stated, the present number and various other suppliers that he had to have been in order to do the hand of whether it is of electronic voting machines or whether it is on your scam -- optical scanning machine. So far you have to be able to identify that to complete your audit. Is really a part thing a bit at the clubhouse to be like that. And we also see in the current session of congress a number of bills that required states to do lots of some kind. Mostly by hand.

And I agree. I guess he took -- this is gales. If you take the sample of the chip the class b taken from the machines and then transmitted to a temporary office and the chip has to be encrypted to ratify the machine so it can be received and identify at the county office. But the issue of whether two people accompany it or four people a company it or what kind of car they drive seems like it is not an issue for tgdc. That is what I distinguish between the two.

I have to say I am very deeply aware of my ignorance in the depths of election procedures so I will not try to read a procedures manual. There is no question about that. If I can to go ahead and talk about the more complicated procedures these are already done. This gives you all the information needed. The second set, we are talking about things that either aren't done or had testing done little bit like parallel testing. This is to verify the machine is being [indiscernible]. Is not carrying out attacks that would be the discrepancy between records. So even though you have a very -- voter verification file paper records machines can certainly the sba. One of the obvious ways that you help it indicates a vote for john and it could print a book for a show on the paper that. There is not the discrepancy between records but just that the voter gets its chance to record -- notice that. If you are blind and not able to notice that you cannot let paper and you either need additional procedural or technical offense to make sure that white voters, have third [indiscernible]. Another issue you have is that you could make the voting machine introduced differential errors. Errors that favor one side or the other. There is a [indiscernible] if you misprint the ballot in little bit you can cause the scanner to catch under votes to cut you look at the same boat for one candidate and not for the other. So the same set of thing where the screen is the slide by mistake and you get these errors. You could certainly said like those errors. That is something you want to be able to catch. There are other things you can do. As an attacker tried to attack an election, even with just paper records being auditing. The nice thing about this is that most of these threats are easy to detect because the voting machine has a misbehave on the side of the voter and there is a good chance of the voter, especially the voter who is pretty aware about the ballot is supposed to look like or somebody who is working in the election or something is likely to notice of there is something odd going on. The problem you have is that when you just have a few people complaining it is not actually clear what you do next. There is no clear place where you can check the two different sets of records or have some procedure were at the end you know ambiguously you are being attacked. I guess that is a pretty, situation. So the other issue is that the whole set of voters who are not able to verify the printed record need some sort of additional defense. That may help down here. One, it is we don't have nearly as much experience operationally but during this kind of thing. We have some experience during parallel testing. Not a lot and observational testing is not something that has been done before as far as I know formally. Okay. We will talk about operational testing. This is something that does come out of discussions about how to employ at the full resolution on software independence periods essentially if I can summarize it is that most software for independence need to work for blind voters and everybody else. So the threat that you have is a voting machine, if there is tapered software piece offer to use the fact you are using an ideal for screen magnifier are something like that as a clue the public will be taking the paper. So it could change your vote on but the paper and electronic record and it cannot take it there is no way for that to be detected. The records will all agree. There is a simple procedure to address this. It gives you some assurance this is not happening which is to have a small number of authorized powers wanted to use the audio ballot for the screen magnifier and to carefully check the printed record. And the goal here is to think about the attacks. The attack program now has to -- it can no longer reliably to change the printed record and know that you can get away with it. So 100 people in the state taking this are very likely to catch any kind of an attack that [indiscernible] a large fraction. And so it is kind of a nice thing to because the actual requirement on the equipment is the equipment to authorize the voter to vote on but the machine has to be something where you don't just hand blind voters a different kind of authorization. This is something we already wanted to do. Okay. Parallel testing is more problematic. It is a powerful defense against the tax where the voting machine misbehaves and

tries to confuse the voters in introducing errors favoring one candidate. The threat here is the voting machine is the [indiscernible] in some way that will only be detected if you watch it carefully on election day. This is not something [indiscernible] final testing. So this is where in the realm of [indiscernible] or in the putting supper on the machine that will this be a only on that day. So we should do testing on a few machines on election day and see if they missed. And of course the requirement is you have to look to the voting machine just like a real voter. So you develop a lot of requirements here, but at a high level has to happen if you want the parallel testing to work is yet to be able to isolate the voting machine so that it cannot get any communication from outside and nobody can tell you -- the person running the tech can tell it, you are being tested [indiscernible]. In the voting machine must take it is being tested. We can go a little further down. We can say if you want to do to cut you want to make sure that you don't isolate the voting machine that means that the glove and machine cannot be talking to other devices in the room. It can't be on the network and that costs problem because that limits be set up possible design. Have some ideas of what you might do in order to support this. But the requirements is to make sure you can do parallel testing. You actually impose some restraints. Things like not being able to get work, the way you do the authorization for voters to vote has to not allow -- it has to be something that can completely take over and there is no way for the voting machine to detect. This is something where we are still trying to figure out what makes sense and we need feedback and discussion in the sts about this, I think. Does it make sense to require support for parallel testing and how much? The last piece of this is much simpler. You have a ballot marker that does not record -- that does not have any memory you can do something a lot more like a traditional testing and just have the voter -- you can have somebody go in and during the election you can cast one test ballot on the thing and get a printed ballot and use procedural mechanisms to make sure that that ballot has been printed out and is correct. The only requirement on the equipment there is just on the a authentication mechanism to make sure that the poll worker does not have some way they can tell the voting machine that is being tested. I think that is pretty straightforward. That is really it for this set up procedures to address in this presentation of attacks. The operational testing is straight forward and powerful. I don't know if it results all the problems with that but it will be something as pretty straightforward. The parallel testing is something where we need more discussion. We need to see if it makes sense to do that. Discussion are questions?

Thank you. Secretary of state here. It seems to create and fabricate all of these imaginative defenses through what seemed to be an issue with source code initially, if we are talking about attacks and not run the box, from what I read in the past minutes it sounded like it is difficult to review source code for a large operation or large system. But what we are talking about in terms of elections, we are talking about a megabyte of code which is what I read in the minutes. I just take it from the minutes. In other words a small bit of information and code. Why is it possible, if we are going to the testing of the source code as part of the certification of equipment, why does it sound like there is such an immense likelihood that you are going to have delicious errors, virus in that code which now we are constructing a lot of difference to deal with? Does that make sense?

I understand your question.

The question. I think that there are layers of defense here and various kinds of threats. The source code review will be imperfect. The source code is just too complicated to get all but there, but the primary concern with parallel testing

is related to the set of validation. The source could may have been manipulated as well. What you have on that machine may not be what you thought you had on the machine. So the question is, is the machine in appropriately for some other reason other than what the source code may have sent?

I guess I have not seen any evidence that any of these things we are talk about have occurred in any equipment anywhere in any system. So we are really constructing an issue here that is how many fairies on the head of a pin, how many ways can you protect against an imaginary foe? The mess there still being maliciously construction of the source code by some people. If this seems to me if we are going to spend all this money on all these back up ways of wanting against source code intrusion, what we just focus our attention on preventing source code intrusion and not all of the variables to prevent consequences?

David wagner here. This is a very long subject. We spent a long time discussing it turns out for independence and we could discuss it again, but to bring it back to kelsey's talk there are many states and places that want to do various kinds of testing with their equipment including testing, conservation and other kinds of testing. So from the point of view of the work that kelsey is doing if it is true that many people want to do this kind of testing than it is important that the equipment be able to support that. Eighty we can have a discussion about the general security issues in general. Maybe you want to do that now or some other time.

I guess I am wondering because of the cost of the testing and certification of vendors to pass that on to all of my counties and every other county in every other state are we building so many redundancies air retry to create a zero error perfection which we have never had an 200 years of our democracy. Is this a new standard we are sitting here with these guidelines, zero error? We will have everything tested to the point with so many redundancies and audits that nobody can afford. But it will be a perfect election.

For clarification, when you say things are expensive like parallel testing is expensive can you say where that expenses in the up front hardware cost? The actual implantation of the test which is the procedure that may or not be done by the states? Where is that cost captured?

The cost that I know of, first of all it imposes restrictions on the design because in order to be able to do this thing where you cordon off the voting machine on election day ideally you constrain the designed is not the machine cannot be talking to the other machines and they can't be on a network. You also impose a lot of cost. Is there anyone here has been involved in parallel testing? You have cost in a sense that you now have to have a testing team go out and do the parallel testing on election day.

My question is, since we are not mandating procedures if the state chose not to implement parallel testing, what is the cost penalty because they had to buy equipment from vendors?

I think the only cost there is, it constrains the design. The vendors will have fewer choices when they are designing the next generation of voting machines. I don't know how to put a dollar cost on that. I have no idea.

This is paul miller with secretary of state in washington. First of all, a comment. I have done some parallel testing in the state of washington. I am concerned on the restraint of the design. I know a couple -- well, particularly the system does not work their devices within the polling place. And they are

able to use a number code as the ballot token instead of having a device, a dongle or a switch or whatever. I am not sure. At this point I think -- you know, we should take a careful look at that. We should see whether or not the benefits of separating machines so that they cannot be network -- would this also include machines [indiscernible] cord as well? Would that include -- would you be putting that sort of a design in this factory as well?

I do not believe so unless there is communication possible over that line. At some point you can start worrying about some global channels where one machine can simply tell something to the other machine, but I don't think that is a big issue that we are considering right now.

And in the hard system where it is a closed loop and in order to operate the individual machines, if you are going to do parallel monitoring you still have to have a loop with a controller device that is connected. And if you randomly select -- I am not sure how -- the equipment, I am not sure how within the closed loop it would be able to communicate that this is test.

I suspect that if you were trying to do this by -- and this is more a guess because I have not tried to do this. I suspect what you would do is test the entire loop. So you could imagine the testing team bringing out additional bad -- a sudden, you know, set of machines and controller at is the way I would suspect you do about. I am talking outside my area of expertise.

I understand.

This is ron. I think this is place where the election officials are important. This is a procedure which is optional by the state. It is expensive when it is done to do parallel testing. The motivation has decreased. So this is language that could be written in there if the state felt it was important to them, but as security devices go it is marginal compared to having the stock -- software independence.

David wagner. I would think that -- to mention on parallel testing, my understanding of how it's done in california is that he set up a mock [indiscernible]. So for those that use precinct its networks I don't think that to be a barrier to parallel testing, but to get to the broader point I would be reluctant to suggest requirements that would constrain the design of these machines in a way that, for instance, prohibit a present base network just on the basis of parallel testing. I think we should be careful here who are drafting and requirements and the states of machines. I think in particular testing is a tricky one and the tgdc should provide input on this particular issue about what, if anything, deserves to be in the standard.

Given the fact that the stock for independent covers the vast majority of what we are talking about call is there a sense that -- is there a body to even continuing to try to drive and discuss the parallel testing options? Is there something we should recommend to the sts subcommittee to move on?

At the election officials be to give their input here but from a securities [indiscernible] of this would be something as simple as the manufacture shall describe what a parallel testing procedure but look like and what is possible.

This is john gale. It seems to me that it was presented as suggestions as opposed to requirements it could be helpful. Obviously there are many sizes of different counties and election centers. So some can afford to spend more money to do more things that others. If these are suggested the idea is at the table

be received favorably, but to try to set one system that's all is not going to work.

The question that is interesting is are there other mechanisms or procedures that eat anybody knows of that address this issue of the voting machines misbehaving in some fairly subtle way that is hard to detect and is not detected in the paper records versus electronic record? And one obvious thing is just to the complaints, but I don't know how you could not put that in the standard at all. You guys know a lot more about that than we do.

Helen. I think probably most election observers go around today and they discover any kind of air that might possibly affect the voting that day. I don't see that is going to be a problem.

So if voters complained you have -- you people at the polling place at the time the bell that and write it down. The question is, how is that addressed later? That is a harder problem.

Well, you not only have the people -- people complaining to the people at the polling place but you also have observers. " they are observing elections. So they will get that information back to you and it will certainly be taken into consideration. In my jurisdiction we have hot lines that the polling places and the trouble shooters are in touch with us all day long so that we know of anything that occurs that they and can solve the problem then.

That is simple.

This is paul miller and I would concur with what was just said that that is the way that counties manage their systems using troubleshooters and hot lines for the polling places. I think you are trying to get at this one thing and I don't know how to get at it yet. The distinction between what is, in fact, a hardware user interface issue and what is, in fact, malicious. Let me offer one example. There is a lot of reports of people saying they touched one candidate and they got another and I know most counties or the counties I am familiar with, if the get a report from the polling place they simply treat that as, the machine was not calibrated correctly of the get that complaint. They shut down the machine and bring out its trouble shooter who either replaces the machine

Do you have sufficient guidance on this subject as to how to move forward on a formal requirements, potentially suggestions or guidance to the vendors?

Not at this when, but further and put as to the desirability would be helpful. And if there is demand for requirements then the machine support that. That would be good to know. If there is not much to [indiscernible] how we can back of on requiring the kind of restraint on the design to support that.

Dr. Jeffrey, john gale secretary of state. Since the hopefully will be issuing their election management guidance in the fall and we don't have them readily available to know whether these issues are going to be addressed because certainly I think this should either be postponed and taken off the table, delayed indefinitely until we have the ability to interface their guidelines with some of these issues because it seems to me that is more a demonstration issue.

That is all I had.

Let me make sure -- given the discussion we have just had essentially we would not anticipate a requirement at this point on the parallel testing. But it may be subject to any additional input at the sts can get from election officials. So with the exception of that issue on the parallel testing do we hear a motion to adopt the rest of the preliminary draft security transparency section that were consistent with the discussion? Is there a motion to essentially be concurrent with the direction they are heading? Subtracting at the parallel testing.

Is there anyone who does not want to second that.

I will second it breaks that me be clear. What we want is the tgdc to formally concur with the direction that the security transparency subcommittee has just presented. The one change is the suppression of the parallel testing as a formal requirement.

I just wanted to make sure I understood. That, we are discussing was that we might include documentation requirements the say that the vendor document how that should be done. But we would not impose hardware requirements? Am I getting what you are saying?

That would be reasonable. No hardware requirements there, but if the machine does have parallel testing capabilities it should be documented.

So if formal resolution. I will propose a formal resolution and I apologize for not getting the english quite right that we accept the direction given with the change that there will be no hardware requirements on the parallel testing, but if a vendor is machine has such that they should document how a state could use that for parallel testing. Is there a second to that motion? There is a motion and it has been seconded. Any discussion or comment on that? Any objections to unanimous consent? Hearing no objection to unanimous consent, we have got that. Okay. Important issues on line. We have to have our priorities straight. So with that I think the security and transparency subcommittee for getting asked about back on schedule. And for teaching us about our cryptography. Is there any other questions or comments before we break for lunch? Okay. If not, let's get back on schedule such that we beat back here at 1:30. Thank you very much for the tgdc members and the you see members. We have a room reserved right next door, diamond rooms a and b for lunch.

[lunch break until 1:30 p.m.]

Please stand by for real-time captions.

If we could all start to move in and get ready for our afternoon session? I'd like to check first of all, um, to see who's on the phone connection. Do we have any members that are joining us for this afternoon?

Sharon turner.

Thank you, sharon. Anyone else ?

The official time is now 1:30, so if everyone could take their seats ?

Just one point of administrative matters. The signer is over on my right. If people want to make use of this, please move over to that side of the room, thank you.

Okay, well, good afternoon! And, welcome back to the meeting of the tgdc. I'll officially call this meeting back to order and I will ask our new to please call roll.

Thank you, sir. Williams? Williams? Williams not responding? Berger? Not responding? Wagner?

Here.

Wagner is present.

Paul miller? Paul miller? Paul miller is not responding. Gail?

Present.

Gail is present.

Mason?

Mason is here.

Gannon.

Here.

Pierce?

Here.

Pierce is here.

Alice? Alice? Alice is not responding.

Purcell? Purcell? Purcell is not responding.

Ravest is present.

Shootser is present.

Turner, billy.

Here.

Turner bouey is present.

Jeffrey?

Here.

Jeffrey is present. We have ten members in attendance.

Thank you very much. And by the way, that's also sufficient for a quorum.

At this point, I think that it's Dr. Allen goldfein and david slater, are you guys up next? And to present the core requirements and testing subcommittee, preliminary report.

Thank you, Dr. Jeffrey. It's goldfein.

You can say it.

Okay, great.

(laughter).

We're all even then.

Okay, great. This is the core requirements and testing report. I'm going to do, let me get to the next slide. There are four basic topics, we're going to be discussing. Electromagnetic compatible requirements, qualita insurance, configuration management requirements, review of the crt changes from the previous draft of several months ago, benchmarks, i'm doing the first half and dave flater is going to be doing the second half. Most of what i'm going to be doing is more of a status report than anything else, talking about, you know, where we've been, what our overall goals are, how close we are to accomplishing those goals, what are the differences between now and this past december, and so on. We are leading up to one unresolved issue that i'm going to toss over to the tgdc for resolution, and i've been told by management to stand up here at the podium until a resolution is --

(laughter).

Is agreed to, or that we perceive a consensus or something like that.

Okay. First of all, the topic that we now call electromagnetic compellability requirements, basically, revision of sections 4.1.2.4 to 4.1.2.12 of volume one of the 2005 vvsg, also this would rerevise part of section six in 2005, namely telecommunications, although from the point of view that we're looking at this, it's pretty much new as far as telecommunications. There really weren't any telecommunications requirements in this area, and as part of the process, they there would also be some changes in testing descriptions, test protocols and so on, a revision of section 4.8 of the 2005.

Basically what we're talking about here is, again, what used to be called electrical requirements, pretty much the ability or the resistance of voting equipment, electrical, electronic voting equipment to be resistant to or, you know, resilient in the face of disturbances, interferences, power surges, that sort of a thing. It's very highly technical. We've talked about it at several crt meetings. We've had discussions outside that on e-mail threads and so on, and it's pretty much, you know, well on its way to being finished. We've divided the area into three subareas, conducted disturbances, basically emanating out of wires and cables and so on, radiated disturbances, electromagnetic signals through the air, and the third area as I said before, telecommunications disturbances. The conducted disturbances section is complete, at least it's complete as of yesterday, probably by monday, I'll be posting the latest draft set of requirements on the web. Radiated disturbances is still being worked upon. As I indicated last time, we've enlisted the experts in this particular area from nist bolder, who there was some delays in that but now they're working hard to define appropriate revisions to the existing requirements, and the telecommunications disturbances which are partly visible on the current draft, still some to be completed. We anticipate that everything should be finished in the sense of having a complete set of requirements for complete examination and integration and development of inform a tivr text and so on, probably no later

than early to mid april, but everything seems to be very straight forward here. I haven't perceived any major disagreements or lack of consensus within crt. I encourage any of you who are interested this subject, if you haven't already, to take a look at the document, well the document that's in the handout and also whatever the revisions are that we continue to place on the web.

The other area i'm going to talk about is that of qualita insurance and configuration management requirements. Our work in this is a response to first of all tgdc res luingz 30.05 which mandated in the sections in 2005 that dealt with quality assurance and configuration management be reconsidered, rethought, in an effort to provide additional stronger, if possible, tools to help insure reliability of voting equipment. This was reaffirmed and extended at the december 2006 tgdc plannary where the tgdc did reach a consensus that yes, iso 9,000, 90001, that family of standards should provide the framework, i'm trying to quote as best I can from the actual transcript, should provide the framework for pbsg 2007 requirements. Of course I guess we're not supposed to use 2007 anymore, but wherever I have 2007 in this presentation, make a global change to whatever is the current politically correct, you know, word. And these revisions, or in this case it's more than a revision, it's a rewrite from scratch of the existing sections would be a replacement for sections eight and nine of volume one and section seven of volume two of 2005. Now, the draft pbsg 2007 requirements, I guess the word draft should be in there, do require that a vendor's quality assurance procedures be in conformance with iso 9000, 9001, and of course in this area, the devil is in the details saying conformance doesn't mean a whole lot. It really comes down to the particular procedures, the particular detailed requirements that are specified. First of all in the vbsg, and then how those requirements are adopted, rephrased, implemented, and so on by the vendor. So what we have now in the draft requirements of the new vbsg , they're more detailed than those of 2005 in terms of vendor, quality and configuration management procedures, that require documentation of these procedures by vendors, data that needs to be delivered at different points in time to the eac or the test labs, what have you, things like that. We've tried to be as detailed as possible without being counter productive.

These draft requirements also require the vendor to specify its quality assurance procedures early in its process, early in its life cycle, not when the product is submitted for certification. In other words, this is generally considered to be important in quality assurance that quality assurance is not something that underlies simply manufacturing but also has specifies procedures that are vital during design, development, what have you. In any case, this particular issue, this particular requirement leads us to the open issue, the somewhat contenc ious issue that i'm going to be macing on the floor here. As I said, a key to the quality assurance success is generally considered to be that the details of a vendors procedures be developed, delivered and approved the appropriate authority before work on a new product begins. A lot of people agree with this in the abstract but what does this mean and how can this goal be accomplished in the context of voting system certification, which of course is a special case and is the specific case that we're dealing with here.

If you look at the eac's certification manual that was published a couple of months ago, the eac manufacturer registration process would seem to be the obvious place for the examination and approval of a vendor's proposed procedures. Now, it fits right in. This is the time when the eac aproves the vendor to essentially go off and develop and deliver machines for testing. Problem though. The eac manual doesn't specify a time frame for the manufacturer registration process. In an extreme case, it could occur the day before the vendor delivers its product for testing. In other words, a vendor could apply

for registration, receive a certificate, and a day later, back up its truck to the testing lab and say okay, here is my product, test it. The problem is that if there weredeficiencies that were discovered at this point, not the product itself but the procedures that were used to design and develop the product, it may be too late at this point to do anything about this problem. It may be impossible to determine whether or not the delivered procedures, remember, here we're talking about quality assurance, it's something a little abstract or above the machine or the product itself, maybe impossible to determine whether or not the procedures were in fact adhered to during the design and development stages. Now, admittedly, I used an extreme case here, but the goal is if you're going to be serious about quality assurance to insure that it underlies the entire life cycle, not just the last stages, the end product and so on.

Okay, so there are a couple of possible solutions we present two of them here. One which was drafted sort of as the straw man is to be explicit and require that the delivery -- maybe I should step back for just a second and be a little clear. Part of this process, part of the requirements require that vendors deliver a manual of their proposed procedures to be examined and a proovred by the eac. What we're talking about really is the timing of this. The first solution requires that the delivery of the qac procedures for approval " shall occur during the manufacturer registration process as specified in the eac testing and certification manual, and before the start of the design and development process for the given voting system. "

This accomplishes the technical goal of insuring to the best of our ability, and there are a lot more details that would be supporting this and so on, but this would solve the technical problems of getting the manufacturer's procedures examined and approved in advance, but the way it's worded, it has the effect of specifying a time frame on this, on the manufacturer's registration process, since the deliver of are is linked to the registration process and the delivery has to be done before the start of the design and development process then it would seem that the manufacturing or manufacturer registration process would also have to be done at that point. This is not something that's contained in the eac manual. It does imply a non-trivial additional requirement on the eac manual, and technical issues aside, this may be outside the scope of the vvsg.

[inaudible].

Thank you.

So, this is why there's an issue here. An alternative is of course to drop the before the start of the design and development process, remember back here, where was it? This clause over here, and simply link it to the manufacturer registration process and leave it in the hands of the eac, kick the ball to them and they're responsible for insuring that or attempting verify that all of this is done in an appropriate time. There could be an informative discussion outside of the specific green requirements in the vvsg that advises that the vendor submission should be done before the start of design and development, as a possible additional bit of information. This of course is optional or remains to be decided, but the problem for this alternative, it defeats the goal to a certain extent, to a large extent of insuring in advance that the vendor has adequate procedures in place before that vendor actually proceeds to go ahead and develop and manufacture his machines. This issue was kicked around at the last crt meeting there was participation in fact from a representative of the eac there, but in the end, the advantages and disadvantages were argued and I didn't perceive that there was any consensus at the end of that discussion. So it was decided to bring it up in front of the tgdc.

I just want to emphasize, this isn't so much a strict technical issue. Is it good or bad to do this as early as possible? It seems to be fairly broad agreement that yeah, sure, the question is how is the best way, the best feasible way of accomplishing that goal, and I sort of turn it over now to a discussion of the tgdc and see if anyone --

Can I have a question for clair any indication?

Please.

Could you, given that in the end, what the guidelines are producing is to insure a certain level of performance, reliability, security, use ability, accessibility --

Right.

For the systems, how it got to that point, how relevant is that? In other words, from your expert opinion on the qacm , mandating the specific process that the manufacturer got to that point, does that add additional value in terms of the outputs that we're looking for?

Well it doesn't mandate a specific process. It mandates some generalities that the vendor looks at and then says okay, in terms of my environment, my procedures, my history, the particular product that I have, here is how I will address these general requirements, and the vendor at that point puts together what's called a quality manual in which he certifies, yes, I will be doing this. Yes, I will follow these sorts of procedures in this particular manner for me. Yes, I will maintain the logs that are required of problems that arose during development, and I will do it in this sort of a manner and so on. Then, this manual, which is of course customized by and for the vendor, is then delivered to the appropriate authority and in this case, the eac, who looks at it and says, " looks good. " it looks as though as best we can determine as best as humanly possible before the start of everything, as best as can be done in a general manner without dealing with specific isolated issues, this looks good. We have proved your quality assurance, your set of quality assurance procedures. The issue, and i'm going to try my best to focus on a narrow but nevertheless what is an important and has many implications is to focus on the timing of this and what is the best way to do it.

If I may, I think that question was a little more general than that. The question essentially was: why do we care that quality procedures are in place in general, if in fact the end result is to accomplish the requirements in the vvsg, if you accomplish those requirements, who cares how you got there which is a philosophical question about the value of things like iso 9000 for instance and I guess that could be debated. I don't know if anyone -- I think that was your question, right?

I'm not trying to raise the philosophical aspect again as to the value of iso 9000, and it's a value and the industry recognizes the value of that but i'm not sure that necessarily has the same merit of requirements in addsg as the output products, but so i'm not questioning the value of 9000 an 9001.

Well if I could just say an answer to that is, well two parts to the answer. One is that it does provide us with an additional tool to help insure reliability. Certainly you can always come up with examples of iso 9000 compliant organizations who reduce garbage and so on, but it does provide one additional

tool, one additional hook that can be used as best as possible to help insure things.

If I could get terry's perogative, I want a clarification question. Is mary saunders here? Well, I apologize, but does nav lab normally look to see whether quality assurance programs in place, is there a precedent under nav lab to insure that once someone goes for certification for final testing that at least some quality program was in place?

[inaudible].

Okay, so the lab does not reach down to see the vendors, okay, thank you.

And the other quick half a sentence answer is that historically, this has always been considered important within the vss and now the vbsg, and we're following our mandate and looking at this. Lynn?

This is lynn. Let me also try to clarify some of this as well. The quality manual is required. It needs to be there. It needs to be built. It does show what the vendor is doing as far as their design and their development and their process. That needs to be there so that the labs when they're assessing the equipment have something that they could say oh, you have all the right processes in place,tedthe idea that the labs are doing this very in hence, a whole lot of extra testing for functionality, for reliability, for security, that will in fact, hopefully, show if there were any problems that may have been designed in, so this is a tool by having this manual. It's just one tool and one extra way of looking to see if something jumps out. What is key is that when the last test a piece of equip am, what is key is that we have a high level of confidence that when they manufacture the next machine and the ones after that, that those machines would be of equal quality and at that same level as the one being tested.

So this is really a question of is it worth having a very strict requirement and one that may pose timing issues? What do we get? What is the benefit of doing that, or is it one of these where it's really you have to submit it, I don't think there really is a question there but it's a matter of vendor beware if there is a problem in your manual , you may fail the testing and the certification, even though you pull it up on the next day. I mean, it's a buyer or a vendor beware type of question, so there's two extremes here.

Whitney?

Whitney, hsp. It seems to me that quality, well, to the extent that use ability and accessibility and security for that matter are qualities of a product, that all of those need to be baked in from the beginning. I mean, if you look at say the fec now eac handbook on developing a user centered system, a system that ends up with good useability, it doesn't say magically do it. It says, you know, there's good established processes for how to do it that are good practice in the field and that should be followed. I find it very hard to imagine how far we could go back to mandate that, having said that while I believe with all of the fibers of my professional heart that this is the right way to do it, in the end, i'm mainly concerned that the end results come out right. And that the work that we've been doing for the past four years has been about determining what coming out right means , and we wrote things like requirements that vendor conduct a test and submit that report in the hopes that not only because we wanted the results of that test and we wanted that report but in the hopes that the vendor would say well i'm going to have to do a test at the end. Maybe I should be

testing as I go along to make sure that the pieces were there, that the end would help hint towards the beginning.

Well of course part of the advantage of the usefulness of a mandated qa procedure is to prevent those sorts of things from happening at the last minute, where the vendor comes in and it's discovered that it is not acceptable, and so on. Maybe if there were a strong qa process all the way through, we wouldn't have gotten to that point.

I have to say, i'm dubious about the ability of a standard to mandate good behavior. I think we can mandate good outcomes but not good behavior.

Well, there is a way of trying and I think the rest of the chapter has drafted or does attempt that and it's a focused issue, a question of timing.

Okay, but then john?

I'm sorry, just a follow-up and I guess this is actually a question for the eac, but the case that you proposed is one in which a vendor arrives at the door of the, you know, with the truck at the door of a testing lab with someone in the back and they are busy submitting their registration documents at the same time. Is there a process by which those documents have to be accepted or is it simply enough as they hit " submit"? Because if there is a process by which they read them and say yes, indeed we deed we accept your registration, it's hard to see that those could happen one day apart.

That's exactly right, whitney. We do have to look at their registration application and part of that is the qa manual and in fact, what's before you now, if you put a period before the word " before" up there, that's in place already. We do everything before that. That's the current practice.

Uh-huh.

So the question really is, just before the start of the design, I think that's really the question before the tgdc here.

And I guess one more follow-up question for allen which is how do you determine when the design and development process have begun?

Well, part of it is perhaps as part of a certification by the vendor that he's about to go out and start doing it. We're talking about slippery here, I mean there's no doubt about it.

I sympathize with your goal. I just find it hard to imagine how it would be --

That's what we've been groping with for weeks now. In other words, the goal is clear but how do we accomplish the goal?

David and john?

I'm trying to understand better the justification behind this. So one answer that I sometimes heard for why one should evaluate process is instead of outputs is if it's too hard to evaluate the outputs to tell whether they are any good, sometimes it may be easier to evaluate the process to see whether the process is good. Is that what you're arguing for here or is there justification a little different?

No. The justification is what is the best way to help insure that the product that are in fact edelivered maximize the probability that they are in fact good. We're still, you know, part of the justification is to minimize the risk, again, whether this is our responsibility or not but to minimize the risk that products come in and they're junk.

Let me try to take a shot at that. If we consider our goal is to end up with as good voting system as possible, not just to pass and/or fail the ones that are bad, the more we build in from the beginning to help insure that happens the better chance we have and at the end, everybody fails and they cannot improve in order to pass, we don't have a good voting system so if we build something from the beginning that does suggest we can do it is a higher probability we'll end up with a better product that's separate from saying whether it passes or fails trying to encourage better products.

Wow, i'd like the center design process for that.

(laughter).

John, did you --

You got to put your patience hat on here with me for just a minute. As i'm hearing all of this discussion i'm thinking of all of the different kinds of manuals that apparently the vendors are going to be either required or by necessity produced. One is going to be a manual that's going to go with the equipment if it is certified and proved, it's going to go out to the election officials and tell them how to use this piece of equipment so that's one manual that makes sense to me. Another manual is a manual that expresses the design criteria by which they are going to produce thousands of these things once it has been certified. That makes sense in terms of quality assurance of the manufacturing process, once it's been approved. But this third one doesn't make any sense to me at all, frankly. If you're going to hand build a porsche and you're going to create a factory porsche, it's created in an entirely different way. You'll have so much more trial and error and ambiguity and indecision and clarification when you're hand building the porsche, you may end up with the same thing in a factory built but the quality assurances and controls are entirely different, even though you may end up with the same end product, and so if I get this, we're saying okay, mr. Vendor , you create this whole quality assurance document with a lot of infinity detail and then you also give us that hand built porsche and I don't know how that quality assurance document makes any difference to that first product, that prototype because that's not how they are going to produce them from then on. So the only people, I can see it benefitting maybe makes the test lab job easier, because they could see how they went through the process of hand building this porsche, and all of the trial and error to get there, so what am I struggling with here?

Well for one thing, I don't know if you read the paper on presenting draft requirements, you know, we don't feel that the quality assurance requirements, we don't feel that they 're particularly owner us. If you look at them, they are very straightforward, fairly general. They do have to be customized by the vendor but it doesn't seem to be a big deal. We're not specifically requiring that there be, this was an earlier issue that there be third party formal certification, you know, an an si certified would certify that the vendor adhere to iso 9000 or anything like that. That would be the perview of the eac to determine its criteria and so on. But I find it, maybe i'm wrong but I find it hard to believe that the design, development, and procedures that were used for the prototype are totally different from the procedures that were used or that

would be used when on the assembly line to produce the production versions. Matter of fact that would seem to be a bad thing.

But when you use a prototype, cost is kind of an open ended issue because you're trying to end up with a product without regard to cost that you can get certified and then you start worrying about efficiencies and economies of scale and how to produce these things so it seems like if we're producing a document that's going to make the testing of this equipment easier, then it's a design based testing, and I thought it was a performance based testing and that's just using my own language, but I thought in the testing process, you show up with this equipment that you hope meets all of these things and somebody tests it and see if it does and it's all performance related but we want to know how you design this thing too.

Most of the vbsg is product based but there are parts and there always have been that are design based. And this is is one of them.

So, um, who benefits then at the end of the day from this document you're talking about?

It helps insure quality, I think the test labs do, and the vendors do. It's a means to help them produce a better product.

Let me just finish a couple comments. I can -- I don't like this gotcha quality that somebody mentioned that you produce this quality assurance document on the basis of one prototype and it can start going through the testing process and if your qa isn't found to be correct , that you fail and you got to start over again, so i'd rather see a qa, if you're going to require qa, that it be maybe something would be filed at the end of the testing process rather than the beginning because both the lab and the vendor are going to learn, aren't they, to the interchange of the process of testing and certifying so that if there are some gotcha in there, they get remedies without throwing you out of the process.

Excuse me.

I'm sorry, I just wanted to clarify and address your comment. There really are no gotchas. The vbsg clearly identifies the requirements of what needs to go into that quality manual, so the vendor knows in advance what are those practices. These are not new. These have been in the standard since 2002 in the earlier standards, many of these requirements. Do you have this section for the qa? I don't.

Yeah. Volume one, section eight and volume two, section seven.

And in fact, all the vendors up until now have created a quality manual that does all, you know, that meets the requirements. We're not really changing many of the requirements other than saying you have to produce the quality manual and deliver it at a certain time. What a quality manual does is it documents a lot or it has the vendors tell us or the labs or the eac what is their process of how they build and design their machine, what are they logging, what are they doing as far as testing and these are requirements that are explicitly stated in the vbsg as well as they have to be able to show that they tested certain of their internal build processes, certain of their configuration processes, they need to be able to log and keep logging certain events and the quality manual is capturing all of that information, so it's not a surprise to them. They should not be surprised by what is expected to be contained in that quality manual which is also guided by an I so standard, so if they appear at the door and

after review, their quality manual has something lacking, that would be a surprise, I think. They should not be surprised.

[inaudible].

No, okay. I think patrick?

It's in the supplemental, the other volume.

Patrick?

It's not in the draft vbsg. It's in the -- there's a proposed, not a proposal but a discussion of draft requirements in that book.

Mary first then patrick.

I have a very brief comment. This is from the perspective of the testing lab and as we look at them. The test lab, you're right, looks at a particular voting system and configuration and does not reach back into the manufacturer's process for producing that initial or whatever its number product it is or the process for purchasing products in the future. It's a one-time test and they don't exercise judgment, they test to the standards. The product system and configuration meet the requirements of the standard, quality management systems are responsible for certification program which is the responsibility of the election assistance commission, whether you can produce repeatable products systems over and over and over again and a very simple point, unfortuntely, the procedure is written as unenforceable. You can't enforce this to require to have a qa manual in place before the vendor starts design development of a particular system, I don't see how you would be able to enforce that.

You can try.

It's already covered in the certification.

You can try.

Ron or patrick?

Yeah, this is patrick gannon. My comment kind of goes to the somewhat along the line often forceability of how this could be implemented. First of all has there been any direct input from existing manufacturers of certified equipment today as to whether or not they feel like sure, they would not have a problem providing such documentation ahead of time, so first question was has there been that level of dialogue to date?

We have not discussed that particular issue with the vendors. A lot of them claim to already be iso 9000 compliant but that takes in a lot of territory, but no, the answer to your question is no.

So help me understand just where is the cm review done and how would having that review prior to the manufacturing or design process, you know, change the outcome? Would they then have to have the procedures reviewed ahead of time, before they start the design process and then after they complete it when they get ready to test their product or are we then having them come back and say okay, you submitted your plan of how you're going to do the process, but now that you've actually started building them and you maybe had changed the process

based upon your own internal testing and qa work, you've now documented, you've revised your manual. Where is the requirement that then gets resubmitted?

Well there is a discussion of that. There is a requirement for how to handle changes, on the fly changes or changes during the development and manufacturing procedures. That is dealt with, but the point is that the earlier that it is done, and remember these are customized by the vendor. The earlier it's done, the earlier potential problems can be identified.

Allen?

I have a question.

So thinking about this from a security viewpoint, I guess the question we're asking is that the vendor may say they are going to run a variety of tests and bring in an external review team for security analysis and run software tools on the code to see if there's any kind of overflow or vulnerabilities or other things, etc, etc, but my understanding is that submitting a plan saying you're going to do those things though in no way committs the vendor to submitting the results of those tests which would be the thing that would be most interesting to say open ended vulnerability testing team or the lab looking at security issues. Is that correct?

What you've just said is strictly correct, that the mere presence in a plan doesn't require it. Some of those things, however, are required by other requirements or should be required by other requirements within the vbsg or within the chapter dealing with this.

The results of this test would be of more interest to the lab than just the fact they were going to do those tests?

You may be right.

Well, I think i'm hearing the concept of quality assurance as a process and quality testing as a part of that process, and I don't know if I have a question here but I want to put that on the table because it seemed to me that what you were talking about was having a quality process, like I just noticed between a user center design process and use ability testing which may be part of that process.

If I understand you correctly, I think yes. What we're talking about is not the testing of the product. I mean the whole rest of the vbsg is --

[inaudible].

It's an additional somewhat separate, somewhat disjoint tool that tries as best as can be done in thismerky area to insure that the procedures and policies and what have you that are followed by the vendor are appropriate and will have the best chance of leading to good results.

So as a clarification, could you give me an example of a part of a qa process that you'd want to see if you were inspecting such a manual?

I think the whole rest of the draft chapter deals with that. There's requirements for logs of problems that were encountered during the the process, whatever it is.

What's an example of a problem encountered?

Well, a lot of this would be dependent upon what the vendor proposed. In other words, if they encountered a nasty problem with some of their software and it took them a lot of revisions to fix this, that might be a fact that the worthy of ultimately being available for observation by the eac.

Okay, if I could, could you go to the slide nine where you have your first, or you have two recommendations.

Right.

As to how to do this and let me see if I can summarize and see if I capture this properly. So your first recommendation would be to sort of force the hand at making sure the quality assurance plan is in place before they start the work which I think the discussion has shown is a significant burn to the eac, may be unenforceable and since we really can't define when design development starts, it's sort of vague, so your second one, basically says okay, vendor, you should, it basically turns it from here is something that we're going to have a pass/fail almost on to this is good practice and you have to submit the quality assurance manual anyway as part of the process. We really encourage that you take this serious when you do it from the beginning and it turns it into a best practice as opposed to a hard pass/fail.

Well even in the second alternative, there is a pass/fail component.

In terms of -[inaudible].

Whenever it is delivered, conceivably a vendor could be flunked.

Yeah, on the second one, this does not have a negative impact on the eac, is that correct, in terms of the guidelines already produced?

No, that's correct because that's the process they have already taken care of.

Right, okay.

Mr. Chairman, john -[inaudible], state of nebraska. For purposes of getting it on the table, i'd move that we adopt the alternative that would require delivery of the qac n procedures for approval during the manufacture registration process as specified in the eac testing and certification manual.

Okay, so that would be what this option is, this alternative option?

Correct.

Yes. Is any further comments or discussions on this?

Is there any objection to unanimous consent on this proposal? Hearing no objection, this passes by unanimous consent. Thank you very much.

And that provides the consensus that I was or a consensus that I was looking for.

And more importantly --

(laughter).

You don't have to stand all day.

Unless i'm called back, yes.

But thank you very much.

Okay.

I appreciate you walking through. That was obviously a subtle issue but actually it has a ripple effect.

Yeah, it has a ripple effect now, all of the reremainder of this issue is fairly clear cut.

Thank you. Now, david flater to review crt changes I believe.

Thank you. If there is -- in the interest of good time management and doing the most important thing first, if there are no objections, i'd like to go to the second half of my presentation first which is about benchmarks. Are there any objections to that?

Benchmarks.

Okay, so this is really the last significant piece of unfinished business from the stuff that i've presented in december. Now, just a quick review, what is a benchmark? Definition: it's a quantitative point of reference to which the measure performance of the system or device may be compared and in plain language, we're talking about the numbers specified in the requirement, such as the failure rate of the voting system shall not exceed benchmark, number. There are three benchmarks that are relevant here. One is for reliability, aka failure rate. One is for accuracy, also known as error rate. And one is about the rate of missfeeds for paper based tabulate ors.

Now, there were some issues that we were left within the previous vbsg. With respect to the time between failure, there was a resolution passed in december to essentially move away from meantime between failure and in addition, there was a lot of public input to the effect of the existing benchmark was not thought to be strict enough so bottom line is we need a new benchmark for reliability.

With respect to accuracy, we found number of ambiguities with the metric as it was specified. There's not necessarily a problem with the benchmark per se, but the way in which it is measured had some issues. The graft contains some clarifications to eliminate that ambiguity and at a minimum, we would need confirmation that the draft of clarification is acceptable. While changing the numbers is also an option.

Finally with regards to the missfeed rate, this is actually a combination of two old requirements, one which said paper based tabulateor, using whatever terminology was current at the time, shall not missfeed in the sense of jam more than one ballot in 10,000. The other requirement which raised eyebrows in the crt committee said that the equipment shall not reject ballots that conform to all vendor specifications more than 2% of the time. That's 2%, and the committee heard that and said, um, 2%, we don't think so. So that's been harm onizeed with essentially those two requirements have been merged under the part of missfeed and to a one in 10,000 benchmark. And that is believed to be relatively non-

controversial unless there are any comments on that. What we're expecting more discussion about is reliability and accuracy.

Now, from the december meeting after a long presentation about the test methods, we ended up with this unfinished business to carry forward, asking for input from election officials to give us the data necessary to derive specific numerical benchmarks to put in the document, meaning okay, here is the test method but what benchmark are we testing to ? The method gives you a measurement and kicks out a number but you need another number to compare that to to determine pass or fail and so given responses to these questions about failure errors and volumes, we could derive those specific benchmarks.

Now, after a period after the last meeting, we didn't seevr input so we sent letters to both n as and n afsed. N as declined to take a position and we did get a response from n afsed which is posted on our public website which i'm going to paraphrase in the slides up come canning. We unfortuntely sort of ran out of time to deal with this issue in advance of this meeting, but we did discuss it at the crt teleconference on the 15th and I have incorporated as much of that as possible into this presentation and last I heard, paul miller was on the line and I think he's going to have some additional comments as well.

Paraphrasing to the best of my ability with regards to reliability: feedback was: no failures that lead to un recoverable votes are acceptable. Other cases are tolerance for failures depends on how hard it is to recover from those failures. There is no " typical" volume in which to base a benchmark. And they proceeded to discuss five categories of reliability and things that need to happen to insure that reliability. As you can see, we have design issues for reliability, resilience to human error, manufacturing quality, maintain ability of the equipment. And the ways in which these are addressed are different, I mean there's a volume test, useability testing, different test methods are applied.

Now, the consequences in terms of the benchmark, okay, we have these test methods that are applicable; however, in order to empower test labs to advise rejection of systems that perform unreliable during testing, there still needs to be a benchmark for what constitutes an unacceptable rate of failure. Again, there needs to be a number with which to compare the output of the test method so even though the right answer in practice depends on many things and we do understand in practice it's very complicated and it's very hard to come back with some number and say that this is a typical volume for an election, there still needs to be a number in the vvsg in order for the test method to be effective.

One option which i'm just going to throw out there, if with ego back to the feedback saying no failures that lead to unrecoverable votes or could lead to unrecoverable votes are acceptable, what would it mean if there were a benchmark of zero? What this would mean is when the equipment is being tested by the test lab, if a failure occurs, the equipment is rejected. We haven't proven that the equipment is never going to fail, ever, but in terms of the practical consequences, depending on the length of your test campaign, it's not necessarily out of the question to specify a benchmark of zero but i'm just going to throw that out there as a possibility and not advocate for it. So with regards to this slide we've sort of come full circle that having examined the feedback received so far, we still need a number. Now there's additional discussion here. Regarding our feedback, our tolerance for failure depends on how hard it is to recover from the failures. We cannot know its certification time with practical impact of different sorts of failures will be because it

depends on the practices and procedures put in place by election officials. Election officials in turn will put practices and procedures in place as required to deal with the equipment that they have. So the argument is completely circular. We cannot determine a benchmark this way. At some point, we need to know really what benchmark is required.

I'm sorry, this is bill. Could I ask a clarification? Because we may be asking, I mean we're asking hard questions for people to give us numbers like what's an average volume and things, but is there any reason to believe that an error rate or that the number of errors will be greater on a smaller volume than a larger volume? And the reason i'm asking that is it would be the bigger the volume, the more errors you would likely have , that you don't really want to specify sort of what's typical but you'd like to look at what's sort of extreme or what's the 95% volume rate, and which there probably is data.

Well, the idea was to derive a rate, and to derive the rate, the way the question was formed was with regards to a typical election, the thought was in a typical election or so we believed, there would be a way to find out what the volume was, and there would also be a way to come up with a figure for how many errors could have been tolerated before we ended up with an unacceptable result. From that you divide the errors by the volume and you have a rate. But in fact, phrasing the question in this way may have caused more problems than it solved. Now, to continue with the feedback, paul miller on the last c rt teleconference was essentially speaking on behalf of n afs ed and saying, what we would really like is to assign different ways to different kinds of failures so that these kind of failures that might possibly result in the loss of votes would be right out but other types of failures that we might be able to rectify on election day or by replacing a machine and recovering the votes later, we might be able to tolerate those. So if we can define these different categories of failures and objectively determineable way, that's what the test lab needs, then we can assign different weights to them and possibly have more complex benchmark, or a benchmark which satisfies the needs.

Now in fact the 1990 voting systems standards try to do exactly this. Appendix gh the voting system failure definition scoring criteria, define the idea of a relevant failure versus an irrelevant failure, and also assigned different weights typically any old failure from which you could recover and continue with I suppose paper jams being in that category, would count as .two whereas something that could potentially end up locking up votes so that you couldn't get them out of the equipment got a value of one. Now, this system was removed in its entirety from the 2002 vs s, and as of the deadline for this presentation, paul miller was following up to find out why this occurred and I haven't communicated with him since. So if paul is on the line?

He's on an airplane.

Darn.

(laughter).

Darn!

Well, this is where we are. Something was done in 1990 vss that once again is starting to sound like a good idea. We want to know why it was taken out. If rick would also know this, probably, but he hasn't made it here either. So -

David let me ask a question and obviously we're not going to wait for paul's plain to land.

(laughter).

From your understanding of appendix g of the 1990, would that really, that methodology resolve the issues?

There are, there is some minor resolveable in compellability for the test method that is there now and I know what I would do to fix them but what I can't do is tell the election officials what benchmark they want.

Right.

Now, based on the old standard we could, if we just assumed that the old standard was correct in every way, we could stick as close as possible to those old numbers. But this sort of gets us back into the old, I mean it was defined in terms of time between failure which we already have a resolution to move away from, so we wanted to rebase this in terms of volume instead of time, so really, the election officials do need to weigh in.

David wagner. If you go back to the slide with your summary of the n afsed letter I believe it was, I wonder if there's some things, some partial things we can learn from that letter. One of them is this distinction between unrecoverable and recoverable failures and I think that's an important distinction. There's a big difference between machine crashes and that corrupts or deletes all the votes and now it's impossible to recover those votes versus a machine crashes and I still have all the previous votes and maybe I can't accept any new voters but I haven't lost any prior votes, and i'm not sure whether I read, i'm just trying to read this on the fly but I didn't see that distinction made in the current definition of failure rate in the draft before us, so I wonder if just starting by making that distinction might allow us to make some progress. For instance, one possible direction one could propose would be failure rate where failures lead to loss of votes, acceptable rate for that might be zero, as listed up here, but the rate of failures which are recoverable or don't have the loss of votes just lead to loss of the ability to service new voters that might be a non-zero rate that's acceptable that could be specified. Also thought maybe i'd just comment a little bit on your statement that this is because we don't know what practices and procedures will be used in the field that's an impossible circular problem, i'm not sure that needs to be such a roadblock. I think that first of all, we can identify there are some failures that are unrecoverable no matter what practices and procedures you use. That is very clear cut what to do. And then I think from there one could look at what the practiced practices and procedures in the use manual provided by the vendor are, and if the use manual that's provided by the vendor supplies practices and procedures tells you to use the system in such a way it leads you to recover, then I think it's fair to classify that as a recoverable failure and it's true maybe there's gray area for failures where the manual doesn't say what to do and we don't know what practices would be used in the field and I don't know what to tell you for the gray area but we maybe able to make some progress there.

If I could respond briefly. One additional complication with regards to recoverable failures I didn't go into and this was among the questions that we asked, we did want to ask if we wanted to have different benchmarks for different types of equipment because if you got one optical scanner counting all of the votes you probably want that to be more reliable than one of the 100 dre's that you have simply because the consequences are worse.

Maybe not.

Okay. That's all.

I think we were on to something here. If you have the right procedures and policy, it's whether there's back up equipment and so fourth, you might even be able to work around non-recoverable failures. I agree that you have to meet something because you have policies and procedures that each municipality might have. And you necessarily want to have the one that the vendor provides also so I would suggest that maybe if you could find some prototype or average kind of policies and procedures that people agree with that is approximately close or representative and you try to do the test around that, then you might be able to get to it, you know, in other words, if people tend to have only one optical scanner , then you test it with only one. If people have only one drein a particular place, you test it with only one. You know, you could follow what i'm saying.

Yeah.

How do you start and recover what a normal kind of procedure? It won't be the same exactly for everyone but there might be some prototypical kinds of policies and procedures you might want to discuss how this would work with that test. Some limit of what the vendor recommends and what the practical people in the field would modify that to.

But then a given optical scanner might be deployed in a p recinct count configuration, the number you have might change, and my intuition would be that this could be like asking about typical volume. That there is no typical would be the answer. So --

This is bill. Do you have a concrete recommendation for tgdc?

Well, actually, it helps you get through accuracy too.

(laughter).

And then I will not make a recommendation but I will say something that will hopefully wrap things up by july. Or june.

Dr. Jeffrey? I'd like to just ask a couple questions of david. And I guess i'm just thinking in terms of election officials dealing with whatever they have, that's their reality and most election officials keep spare parts, spare ink, spare cartridges, things that they can deal with and replace, so if you're running out of ink or if an optical scanner is getting too much dust on the light so that it's not reading properly, they can step in and clean that off and recover the equipment to continue to count. So there is so many things that in some ways you might call a failure, but it's a very recoverable issue on a lot of levels as long as there's some training and they have spare parts and that's one level and then you have the level of well, maybe there's a bigger problem and you have to have a technician come in but then the machine is not going to be put back into storage because the technician is available and can address the issue. So I don't know if when you talk about failures outside of that context, whether ever prix precinct usually will have two pieces of equipment anyway and so even if one is down, it doesn't mean that the election can't go on. It doesn't end the election because the other piece of equipment can be used or you can do ballot on demand and print p a paper ballots, so when we talk about

failure, we talking about failure of the election or just an in recoverable failure of the piece of equipment no matter where there's back up equipment to step in its place or not, so I have trouble with this issue of what kind of failure are we measuring.

Perhaps I should have started with a definition of failure. Anticipated events like running out of paper, running out of ink, having to sweep the dust off the sensor, these don't even register on the radar. These are not failures. These are expected maintenance chores. Unexpected thing like a paper jam is probably the least severe thing that qualifies as a failure, and it gets worse from there.

Now, the issue about recover ability, even in the old standards there was a requirement to the effect of not having a single point of failure and things like that. An argument could be made wherein fact we could make it so by adding unambiguous requirements that the notion that any equipment should fail in a way that makes any vote completely unrecoverable is already a non-conformity regardless of the reliability benchmark. And that would take that out of the equation, and then we would simply be focusing on everything in the middle, okay? If unrecoverable votes are completely banned, replacing the ink is come preetly in rel evarnt, then everything in the middle is a failure. And those are what we count for the sake of reliability benchmark.

[inaudible]. How about a scenario where we're feeding in optical ballots about one of them gets chewed up?

Well i'm just repeating what n afsad told me.

Yup.

No failures that lead to unrecoverable votes are acceptable. That's one thing I have in writing.

[inaudible]. This is one of those cases where what it says in the standard may be something that in the real physical world may not be enforceable but the consequences in the test lab are that if this happens when anyone is watching --

(laughter).

When the equipment will not be certified.

David? Since think isn't a concrete recommendation at this point because it's clearly more work, but I think that there's a general sense that dividing up the failures into the non-recoverable and recoverable, there's maybe something in there that looks good, and I think that seems to make sense to a lot of people.

Yes. And we need not go as far as instituting the scoring system from1990 if there was a reason for taking that out which we're still waiting on but certainly making this division as a simple enough thing to do and everyone seems to like it so great. Can I move on to accuracy now? No objection?

I'm paraphrasing n afsad on accuracy, something that I found myself commenting on on many occasions talking about elections past and future is the real requirement on the voting system is that it have one less error than the vote margin between first and second place.

(laughter).

That's the real requirement. Now, if we get beyond that and okay, so what's the benchmark ? The old standard said one in 10 million ballot positions was allowed to be wrong, and this was a compromise based on testing and of course the cost of testing, you can't of course prove perfect accuracy in any length test and on the surface, there's no reason to change this benchmark, but there is need to review the test methods as I had mentioned earlier, there was ambiguity with the metric because it was specified.

They also expressed some concern that the one in 10 million ballot positions benchmark might be achieveable for perfect test ballots but maybe not for real ballots. Hmmmmm.

[inaudible].

Um, it depends I think somewhat upon the voting equipment first of all, so let me illustrate. You talking about a dre piece of equipment and then short of it breaking down to failing or being compromised, it's going to be accurate. If you're talking about an optical kind of a thing, then yes , you may have accuracy problems but short of the illustration I gave where just gets chewed up and not re cover canable, you could design it so that you make as high an accuracy as you want and that system is unable to with that confidence provide you that output and then it kicks it out for a human being to look at so the accuracy could be somewhat influenced by the mainer in which the system is designed and used. If you follow what i'm saying? So I think you just have to factor that in also. It is somewhat related to the procedures and selected guidelines, if you this there's problems in the accuracy not being as good as you'd like in the optical, you could actually compensate for some of that if you were to adjust it for yes, no, or maybe.

Yeah. And I talked a little bit about marginal marks in december. This is a -- it's a call it pwraiingz item for optical scanners. And at that time, the issue was that in fact, you do want the capability for the system to reject ballots that contain marginal marks, because even though your call it pwraiingz may be this way or that, as long as you have this maybe zone to find, okay? Above here, you're pretty confident that it's a yes. Below here you're pretty confident it's a no, and the rest might be below the noise at some point and that's what you want to kick out.

Right.

Certainly using that practice will help you, certainly in the precinct where the voter is standing there and can be asked to clarify, I don't know what you'd do in the central count case or an absent tee ballot. Have you to arbitrate.

You have to determine what they thought --

So, with regards to --

If I could, for a second. The accuracy also depends upon the end-user of the product and that's where you get into what you were talking about, your absent tee or early ballot the because you can't determine that there was something wrong with that ballot. For instance, if somebody instead of marking an arrow circles something but it doesn't go through the read path at all, the machine doesn't pick it up because the machine doesn't know it's there.

Uh-huh.

So that's something, if they do everything on the ballot that way, it comes out as a blank ballot so you look at that , but if by some chance, they didn't do everything on the ballot that way, there is some error of mark in there, so that accuracy is going to depend on what that user does with the ballot.

And in this case, questions of deriving voter intent from ballots where they completely ignored the instructions is sort of out of scope. This discussion is about ballots where or that conform to the requirements. This is a properly marked ballot, and we want to know how often does the machine make an error on a properly marked ballot?

So you're not looking at an error made by the voter?

No.

But merely an error made by the machine.

Yes.

In reading what the voter put on there?

Yes. So that rate should be low.

Right.

So, continuing with the discussion of the benchmark based on the feedback received, the vote margin criteria, yes, in real-life, we would always like to have the number of errors be less than the vote margin, but since you might get a vote margin of one or even 0, that's a perfectly possible, if unlikely scenario. That doesn't help us to set a benchmark other than zero, as I said before, zero is a possibility.

Now there was some support given for the one in 10 million ballot positions number, but with then if we move forward from that as a starting point, the clarification that I discussed in the draft in december was moving from ballot positions as the basic from the method to something called report total error rate and this has to do with the fact that what you're getting out of the system is a report and actually, if you go back to the 1990 spec, it was sort of it started way back then between ballot positions and votes, and what you're seeing in the reports is not ballot positions. It's votes, and the benchmark was written in terms of ballot positions but then the evaluation about what you do when you see errors was written in terms of votes and looking at the reports, so there's a bit of a confusion all along on that, and the draft currently addresses that using report total error rate is looking strictly at votes instead of ballot positions. Having made that alter asian, it's worth revisiting in one in 10 million number to ask if this is still appropriate because it will have some impact.

Now, perhaps more worrysome was the comment about the achieveability of the benchmark for " real ballots". The implication was that for some category of real systems, where was it? Only perfect test ballots are going to be able to accomplish one in 10 million and that if you took a stack of real ballots from real election, you won't make that benchmark. If that's the case, we have already discussed using volume testing with real people and real ballots. There's been a lot of support for doing that as part of the test campaign. If that's what we're going to do, then the benchmark should be something that's

achieveable in that context, unless you want to disqualify everyone. We don't have that figure. So once again, we're sort of asking what error rates are being achieved in practice, and I believe there's some comments.

John and whitney. Well, i'm just sitting here thinking about equipment that maybe has a maximum use in a precinct of maybe 1,500 voters and maybe will be used a maximum of six times a year and so maybe you're getting 10,000 real votes real ballots cast on that equipment. If you have a ten year lifetime your talking 100,000, so this one in 10 million just doesn't even begin to make sense to me as an amateur in this business when in terms of the reality of the equipment, it's dramatically less in terms of the expected use, ordinary use, and obviously you'd need a multiple of that of somewhat, but I don't see what the options are, if one in 10 million makes sense, of course it doesn't make sense to me but maybe it makes sense in terms of science, but it seems like you're testing equipment way too high a degree of perfection that's going to drive up costs and going to drive up the inherent ability of election officials to buy new equipment if we test this to perfection which is what this sounds like to me as opposed to the reality of how the equipment is going to be used.

My question is actually related and I'll eliminate the part that overlapped. One of the questions I have between sort of machine testing with perfect ballots and volume testing sr we thinking about having both of those because one of the things i've seen done in other context is that you use a fairly stringent perfect world test which is cheaper to run because it's a sort of machine test before you go into something that involves lots of people which there for becomes a more expensive test to run. So you can use that for is it mechanically sound enough to go on with and so at that point, you tend to get requirements that are more stringent than real world because then you're also going to go through a kind of real world environment.

I think we're talking about a couple different things so maybe we can dissect it. One thing for volume testing is just to find out if the system will holdup under a lot of documents going through it or a lot of votes and what's going to happen to it as you start beating the system with a lot of volume. The other figure that you talk about with real people is you're also introducing particularly in the case of the optical scanner, the fact that the people may not do perfect circle the and so fourth. So I would suggest that maybe we could separate those two types of tests. We is we could feed through lots of perfect ballots to just see how the equipment holds up and under that kind of volume from a reliability sense and another as we get some proto typical samples o of what real ballots are and see how the equipment operates under variability and how real people do the ballots, but don't submit that to the volume test. We're really trying to just see the kinds of things you're talking about, circle and not full circle and so fourth, filling it in and see how well it works there and come to some conclusions.

Stress testing is in fact a separate item. And you don't care necessarily, I mean, you're not going to achieve the full volume desired when you've got human beings in the loop, so stress testing can be performed validly without people in the loop. And that's written into the language now. The language is rather general about the series of different types of testing that are done but that is a separate type of testing from, it's really only called volume testing because of the california volume reliability testing protocol which is where this idea came from. In reality, I mean, if we had to pick a better name for it, it would be something like real people testing.

Right.

Realistic election scenario testing. David?

Um, I want what secretary gill said that one in 10 million number is artificial and doesn't seem to have much bearing to the real world performance of these systems and I don't think there's any reason we should feel constrained to stick with that number and I think what you're proposing here to base the error rate when it's marked with real ballots under conditions where people are filling them out, that we hope will be representative of how we'll actually be used in the field, I think it's a very positive direction and yeah, I agree this is the stumbling block because we don't have that figure, but it's that figure of what's achieveable turns out to be a much different number from one in 10 million, even if it's one or two magnitude different, I think we should just accept that and that will be a very positive direction. So I know that's not very helpful to say other than I think this is a great direction you're heading. I don't month how to help you go there further.

(laughter).

And at one-time before we had a discussion about optical stuff, some kind of a half way solution. In other words, let's say I had a machine which was a dre kind of machine but it's not recording any votes, it's not storing anything electronically. I'm just using that to drive a printer is what i'm saying so some of you could come up there and see the ballot on the screen, make their choices, and then it drives the printer which produces an absolutely valid perfect kind of a ballot every time, that might be a device you might want to think about.

That's a class of devises called ebm's electronically assisted ballot markers.

Right. And that ends up providing --

Better accuracy and everything else, you'd want to know that and convey that to people in the testing.

Well in fact we want to set a performance benchmark and not pick winners among the designs.

Yes.

If we set a benchmark in some particular design, can't meet it, well that's too bad, but we want to set a benchmark that will be designed agnostic.

I just wanted to support the idea that one in 10 million seems awfully high to me. Voters of the most notoriously inaccurate part of the system here in getting a voter to be accurate with a better than 1% error rate is probably impossible and some of the studies seem more like 3-5% is more common so if you have a system which 1% is inaccurate, I think you're down on the noise so one in 10,000 would certainly probably be fine, and if we get one in 100,000 as a target number, I think we would be in good shape.

(laughter).

This is bill jeffrey. Secretary gill, is further echoed by david and ron. For the volume testing, obviously to what we really need is sort of paramount. You want to get this as efficiently as possible but be realistic and I think john's back of the envelope calculation gave reasonable numbers, I think one could go

and actually get that kind of data to look at what are reasonable volumes that exist out there and you've got all the statistical powerhouse that you can with itl to figure out a cost interval and the testing to come out with some reasonable level of assurance that again, one in 10 million is sort of doesn't pass a test for volume testing, but something maybe more than a few percent, but less than that, I mean, it seems like there should be a way to do it. My guess is by going out and continuing to canvas people's opinions on the matter is not going to be as productive as actually doing the back of the envelope calculation, coming up with what you think is reasonable and justifying why you think that's a reasonable number and then letting people debate the reasonableness of your assumptions. Otherwise you're going to continue to get circular arguments.

Well, not being an election administrator I don't have a lot of confidence in my back of the envelope estimation of the achieveable error rate. The bottom line is there is --

But maybe pars the problem differently. I mean, secretary gill, if you looked at just the number of times the ballot is going to be cast on that divisor the number of types an optical scanner is likely to read that, that gives you some upper limit essentially for that and again, you know, those were numbers just from experience but my guess is that there's something that you can get from some of these groups as to how many times a typical machine does see a ballot. I think you can probably pars the question into something answerable. All right, I have increased specificity of what the question is and that can then drive some of your assumptions.

Okay.

Dr. Jeffrey, I think i'm going to have to clarify what I said because I was thinking of precinct scanners. When you get into central scanning, the m650's you're talking about a much faster processing and a much higher number of ballots that the do get processed per piece of equipment, so I guess we do need to clarify at least in terms of optical scanning, are we talking about really big ones or the precinct ones?

Well I look forward to getting back in touch with paul miller.

(laughter).

Who also should have perhaps some of these back of the envelope figures. I would encourage everyone with an interest in this to participate in the next crt teleconference and let's reach closure on this to the best of our abilities. Bottom line is right now, we don't have the number and we need all relevant input, now! It's not yesterday or last month.

(laughter).

What's in the draft now? There's a number in the draft now, but if you want me to do a back of the envelope justification for it, it might be doable but it will be far better if we have absolutely everyone on board here, everyone needs to nowhere the number came from. We obviously have a problem with the 10 million, okay? That's been in there since 2002 and people are still being surprised by it. So we don't want to do that again.

To clarify, just reaching out and asking people for numbers, i'm not sure what you really are going to be end up being able to do a with that. The number is 42.

(laughter).

Yeah. I gather that I asked the wrong questions.

Well what i'm suggesting is that you, perhaps, outline a specific methodology, populate it with your numbers with the assumptions and allow people to then take each assumption and argue what the range of those numbers might be that can get you there. As opposed to just the end state being the number one in 10 million or zero.

Well, here is is a thought. There are -[inaudible] out there in the field that people are using right now, so supposing I were to take some of that equipment in the field, on the even ideal circumstances in that, it's not out there, it's calibrated before it's done and so fourth and I run that machine and it's actually being used under some of these tests and to find out what numbers they actually are achieving and that's an ideal situation for that machine. Now it may not be satisfactory from one vote, but it had to be one in 10,000 but that's at least a number you can have as a benchmark and they should be at least as good as what the out in the field today and of course, we start finding some equipment can actually produce superior numbers, then you might want to consider some time changing that number but at least it's saying that what municipalities are using today, the new equipment to get you should be at least as good as that under the same kind of tested conditions and maybe that's good enough. It's not where we would like to be but that's what's being used. So you might think about that as to actually have someone test it.

David?

Um, a possible constructive direction that could help you committ a number would be just to elaborate what dan is saying, there are a number of states that have been doing audits of their voting equipment and one possibility could be that may be possible to gather data on the results of those audits, for instance helen sents in a document from her county reporting the results of the audit and there were a couple of cases in there where you could identify how frequently errors and how the scanners interpreted the ballot occurred, in my state of california does audits and many states do awd its so may be possible to get some data that could help guide you as well.

I was going to foup up on what Dr. Jeffries said. He may not be comfortable with the number but would you be able to construct the formula? If the formula is one and n and the n is derived by a calculation by what secretary gill just did, then you really argue the input to the formula and not the formula itself and it's interesting to do both things, to think about how you would decide that is the formula get input on whether that formula is a good formula, and then ask what the numbers that are input into that formula should be which is a second issue.

Well, in terms of the test method, what we discussed in december was we didn't want the formula to be based on time.

That's correct.

And the suggestion was to move towards a volume base.

No, no, correct. Secretary gill gave you an off the cuff volume formula which was well this many voters, this many voters, this many elections, this many years of service, and if that's the right calculation, x times y times z, then the only question is what are those numbers and out pops your one in what number?

Yes. I agree. That's just another way of deriving a number.

But what i'm saying in terms of what question you ask to get meaningful input, you could construct that formula, show an example and then say, and what are the numbers here? Is it ten years? Is it 20 years in service? Is it one election a year, is it six elections a year? Is it five voters per election, is it 100,000 voters per election? Those are probably two outside extremes so that might help you narrow in on the number, because the number is really a product of a number of other numbers.

I will accept all constructive input on what the right questions are that I should be asking

(laughter).

Well, there's mine.

You have the right quality assurance documentation --

(laughter).

I'm sorry, I missed that.

Um, okay, well, if i'm done with this, then that leaves me three and a half minutes to do the other half of my presentation.

(laughter).

Keep going.

Okay.

Well, in fact what I have to report here, i've presented a whole pile of new sections in december. I don't have any have any sections to present this time. All I have is sections that I presented in december. I will point out two significant issues, one already is with regards to the benchmarking test method and the benchmarks themselves. .

There will be a brief pause while captions transition. Pl
The document title review of crt changes. This is essentially a change log against the sections that I presented in december all of the references to volume 2 section anything are off by a few chapters because a bunch of chapters were submitted after this went to print. What I would say is perhaps-- I don't mean to-- to push the agenda around, but perhaps the best use of time would be if people care to examine this three-page document, well, four-page document over the break at some point, if there are any questions about it afterwards, I could take those questions, but otherwise we can move on the the next. Would that be acceptable to everyone? All right. Thank you all.

Okay. Thank you very much. For the preceding presentations on the core requirements and testing subcommittee, actually my notes respond to eight relevant pgc resolutions, and unless there are supplemental directions and corrections above and beyond what we already discussed, do I hear a motion to adopt their requirements testing section consistent with the discussion? Other words that they are basically on the right path, except for all of the unknown numbers.

So moved.

Okay. And second is moved. Seconded. Any objection to unanimous consent. Hearing none, we'll only 22 seconds past the time for the break. So we'll catch that up. Thank you very much.

Okay. I'll give my three-minute warning. To three minutes to wrap up the break.

Okay. It's just about 3:30. If everything could take their seats and all of the people ignoring me in the back. That includes you.

One logistic item, while everybody is sitting down, for those that are planning in the audience to take the shuttle back to the metro, the last shuttle is at 5:30, so we're planning to wrap up around 5:30, hopefully a little earlier, but you probably want to leave here if you are going to get the shuttle at around 5:25.

I will wait 30 more seconds for people to wander in from the hallway. Okay. At this time I would like to ask sharon laskowski to present human factors and privacy subcommittee preliminary draft report.

Okay. Thank you very much. Good afternoon. So I don't know if I eel take the full two hours, here, but you never know. There's always some interesting questions that come up. Okay. Quick overview. I'm going to talk about four topics, first some changes and issues in the-- that have come up in the hfp section. Some issues that require further analysis, then I'll give a little tutorial on how we're developing benchmarks and what the status is of-- and our progress. You have already got a bit of a a tuer toal from david flater. There are three significant changes from the december meeting, and I'll used to the requirementing using the chapter 12. There were lots of other editorial things that did not change content, so i'm not going over those. Okay. First one, in [indiscernible] 05 we required the availability of different choice of font size and contrast on the accessible voting station. And because when we looked at what is currently commercially available we realized that just about all of the voting stations do allow this kind of adjustment, so in aligning with our-- one of our very first resolutions at the first meeting we said we ought to just require that on all of the voter ed itable ballot devices that are for the visual, so we moved them to section 2 of chapter 12. So we now have available font sizes under the control of the voter. You'll note that one thing that we also allow is that second sentence, the system shall allow the voter to adjust font size throughout the voting session while preserving the current ballot choices. We also moved the high contrast for electronic displays to the usability section, and again, the voter can adjust this throughout the voting session. So our suggestion is that we should remove the requirements. We'll put a pointer in there, in both-- forward and back to remove it from the accessible voting station because it's redundant, because all of the usability requirements pertain to all voting systems and we also-- and we-- we look through all the adjustable controls of the voting station, and we updated for them to be available throughout the voting station, so we have got general adjustablety for

all of the requirements when the voter can control or adjust some aspect of the voting station, that can be done throughout the voting session throughout loss of information so for the most part that was already in there. There are two that are new, because as I said we revisited and looked through all of the controls that were possible. One was for the sing row niced audio and video. That changed there. The voter can choose either audio or visual output or both. The idea being that for-- if you are blind you just want to hear it and preserve your privacy and you want to shut the video off-- if you don't need the audio, you don't want to listen it to, and if you have certain concentrating abilities you might want to hear and see at the same time switch among the three modes throughout the voting session. Similarly we did the same for voter control language that the voter can select among the available language, so now we have got the same parallel construction for all of the controls. Any questions? The second irk you-- this was discussed in our previous meeting. We re-- we had-- we were given the safety requirement from--

Can I ask a question about the previous slide.

Sure.

Sorry to interrupt.

No problem.

Voter control language this will allow the voter to select among the available language-- so everything on the display screen-- if the voter requests to see english for the first part and then french later on, when that go to the review screen what happens?

If they decide-- I'll use my example from the hardware store where I accidentally hit spanish and couldn't read anything and couldn't change it back, if they decide-- for the review screen they can have either language.

So it's not the language they requested earlier--

Right. Maybe they start off in english and they said i'm confused now. I really need to see the spanish version. So they can do that at that point.

This is whitney. One of the things we heard and observes is that someone who is a two-language speaker might start outgoing to the candidate race us happen illy voting for president, senator and so on and again get to a complicated ballot question and want to be able to read that at the second language. And to be able to switch at that point-- of course the names are always what they are so that doesn't change.

Okay. So in an earlier version of the vvsg from the last meeting we referred to osha as the insert of umbrella safety requirement, and we discussed this with several nist people who are experts in osha regulation, and ul60950, and they explained to us that the osha reference is a regulation. What we really wanted was the actual safety standard itself, which indeed is ul605950 and that would be the correct way to refer to the safety regulation. Okay. Well, I said that was the third issue, the second one was general adjustablety throughout. Okay. So there-- there are several issues that we have looked at that require some further analysis, some are thornnier than others. I'll go through them. I'm going to actually give a little tuer toal in a moment. We have required by vendor, but what would be very useful is this is a very general test reporting format that we refer to as we would like to specialize it. For xfrp xafrp. In

your benchmark we have developed a verification of a user satisfaction questionnaire specifically for for voting. So there's no reason why we can't provide that and save a lot of headache in trying to figure out are there any standards throughout? So we can do things like that at would at least like to do that for the general usability test that a vendor would submit, but there are several others, and I think that's a little longer term. Research is just providing guidance on how to specialize the sts, and just to make that more sense I thought it would be interesting to give a quick two-slide up ought to ore. A it describes how to report, not what to test, but how to report on a usability test. The focus is to give a point in time, what is the usability of a particular system? That is-- is what we call similar mative usability testing, and the original sufficient of the sif was to have a different format so different organizations could review and compare results. We think the same logic applies for looking at vendor reports as well. It's easier to read them if they have the same look and feel. This is an iso standard. I have cut be its and pieces. For example, the test objectives, and in this case, we-- when I talk about specialization of the sif, we can give very specific test objectives here, because it's for a voting system, and-- other things that get reported, so the number of participants, and there's some guidance as to the minimum number of participants that should be reported. Of course you have heard about our usability metrics, satisfaction, which comes from other standards. So in general-- and I bring this up, because I want to talk about it a little later when I talk about usability test, and this gives me a little framework to talk about it, the actual users in the demographics, the environment, the working conditions so for our voting benchmark tests we did do a think aloud because we're timing, and we just wan the voter to vote on the machine. You often make a decision on whether to provide assistance or not. Measures of effectiveness can be completion rate, number of errors, et cetera, and as I said I bring this up because I didn't want the sif to be mysterious. It's pretty straight-forward reporting. So that brings me to this research issue of performance metrics. That is, you'll see in 12.2.11 we have no numbers at this point, but we have made some progress. I'm going to talk about that in a moment. But that is an open issue right now. And the next issue is based on our discussion from the earlier meeting of end to end accessibility evaluation, and in the vvsg glossary there are two deafnations for end the security definition which is supporting voter and election variation and more generic covering the election process. So end is end is this more generic process. And that's what is in the glossary now. If there is an issue with it, we can certainly alter it. So when you do accessibility testing of the components in the standard itself a lot of them are designed guidelines, requirements, and even if you do some usability testing with a particular set of voerts, just on the voting station, that's not necessarily sufficient to ensure the entire voting process is successful; that it does not violate-- that is the end to end provice cess-- our goal here is to create a place for-- in the standard for test methods to ensure we have looked at how the whole process fits together. So basically wa we're going to try to author is a fairly simple requirement for our system to support end to end process accessibility, which will then be demonstrated by an end to end comprehensive evaluation. That doesn't necessarily have to be with users. If you have a knowledgeable accessibility expert, one could do a walk-through of the system if they are knowledgeable about what some of the pitfalls are. But second part of the requirement will be the vendor shall document the process by which the system supports the end to end accessibility, so the test lab could use that documentation to confirm that the end to end accessibility does work. Any questions about that? Okay. The next issue they just want to put on the table. We're going to have lots of time to discuss this in detail tomorrow under si and accessibility, but I wanted to put on people's radar screen, there is some very early draft wording. I don't know the outcome of our discussion tomorrow, so I

don't know if this is going to make sense after that or not, but it's a starting point. The accessibility of paper-based vote verification. In the station generates a paper record or some other readable record for the purpose of allowing voters to verify their ballot choices then system should provide an mechanism to generate an audio representation of its content. This should be accessible to voters with accessibility issues. I just wanted to get that wording on your radar screen. Any questions? In-- in our-- our travels through editing the hfp section, we note the vvsg '05 dexterity requirement that if the voting station supports ballot submission for non-disabled voters, than it shall provide feature thaens able voters who lack fine motor control or use of their hands to perform the submission. This is also going to be talked tab in some detail tomorrow. So we recognize privacy is important. And for people with dexterity issues, there's been suggestions and some ability to use a privacy suite to preserve that. But this requirement goes beyond that and says it also requires as in shall, independence and this does have implication for electronic ballot markers and precinct count optical scanners, because i'm not aware of any systems-- commercial systems that do inneed address this. So again, I want to put this on your radar screen, because this issue will come up again tomorrow in the accessibility discussion. Probably will also require some discussion with the eac as well since this is in the current version-- the vvsg '05 version.

You are requiring this of all voting machines or some special machines that could do this?

This is for the accessible voting station.

Okay.

Right. Right. Okay. So that's-- that completes my discussion of the issues that we're currently chewing on. Okay. So I want to talk now about where we are with our usability performance benchmark issue. And our overall goal is to have quantitative benchmark requirements for usability with confirm mans determined by running usability test with typical voters, so here are the steps that we need to do to get to that point. Develop a test protocol and metrics. I'm going to talk about that in a moment. Show the test is valid. We believe we have stheed showed that our test is valid. Show the test is reliable this is the next stage of our testing that's going on right now. By that, I mean, that we can reproduce it, and repeat it. That is the same-- testers can-- let me get this straight-- can reproduce-- no, reversed it again. I always do this. The same set of testers can repeat it and get the same results, and that another test lab can perform that test and get the same results. Next step is to test a number of commercial machines, so we get an idea of what their performance baseline is for this test, for this specific test protocol . Some of the issues we're in the process of dealing with right now is how do you do this cost effectively? Because we want large enough number of voters to ensure statist I will significant results with-- and we want tight confident intervals. So I might say I ran this test with 10 voters, and 8 out of 10 completed the ballot out errors. That's binary, yes or no, did they have a perfect ballot, for -- so I ran it with 10 voters, and 8 out of 10 had-- produce a perfect ballot with our test protocol and our test ballot. Or if I told you I ran it with 100 voters, and 80 completed it successfully with a perfect ballot. You would have a tighter confidence interval. We're trying to find out-- to balance enough voerts to get a good tight confidence interval but not thousands of users to make the test too costly to run.

[indiscernible].

Microphone, please?

There's another variable too. If I did it with-- let's say a very homo genous population--

I'm going to talk about that in a moment.

All right.

Okay. In fact-- i'm going to make two statements about that. There's two aspects about that. I have been thinking about this for a long time. Okay. So and there's different ways of counting, and that determines our metrics, so which ones do we want to use? And what is the statistic treatments of these metrics to determine the confident intervals. So we have been working with some of the nist top statisticians to work through that because i'm not a statistician, and at that-- at that point, we can then by looking at a perform baseline and how we calculate that performance baseline, we can then put in our benchmarks. Okay. So this is sort of an informal description of our test protocol, because I thought I would try to make this more concrete for the committee. So basically we recruit participating with specified demographics so in this initial test round to determine validity, we used a rather homo genes you group of people that we expected to get performance on to see if we could distinguish between different systems, and I'll give you-- talk about that a little more in a moment, but obvious I will for a larger test you want to-- participants with demographics that are relatively representative. It doesn't have to be entirely representative, because we're testing something in a lab. We want enough to generate the different kinds of errors that one would expect to see, and we have a meeting complexsy ball loed, 20 contents and rev ren da. We ask vendors to implement that test ballot and to show off some their-- [indiscernible] best light. And we follow the-- the test administrators follow a script. The participating are told how to vote. Make it look like this. To make 28 entries. No assistance or training is given. We say here is a voting machine whatever is typical training materials provided around the machine, that's what they see. We measure errors and time to vote, and basically those errors are differences from what we expected to see, given how we told them to vote, and whether they were able to cast or not cast the ballot. And we administer a questionnaire. It's a modified survey of users, that's widely used in the industry. It's basically 10 statements, it's a five-point liquored scale. Things like I felt confident I used this voting machine correctly, I felt like I would need support, I felt like this was easy to use. And this have been validated in a number of different contexts.

Whitney?

Just to clarify, could you-- I suppose I should say the answer, since I know the answer. The ballot you constructed was that using real candidates and real porties?

No, we tried not to bias things, so we used different colors for parties, and we made up names that looked like real names but had no relation to any candidates, just out of the phone book. [indiscernible] actually used some software that generates random names, which would be another way to do that.

One of the things we're reading is trying to use a real ballot, you get people who say, but I don't want to vote the way you instructed me.

Exactly.

Was it just for candidates--

Yeah, there were three--

There were six contexts that were yes, no type--

Yes, and I think there were three actual wordy rev ren da. We had 47 test participates, high school through college degrees. We wanted people who were perform reasonably well and we had had two different types of voting systems. We wanted to ask the question, do we find errors in this group, because then for sure-- and do we find-- if we can find it with this group, that means we can test with smaller populations because for sure we're going to get the whole spectrum of errors and we got the kinds of errors that we predicted. Does the test detect differences between machines? Is another way to look at value didty. Does the test measure what we want to measure? And we did mooind find there were differences between the two different types of machines that we used, and are those differences realistic differences? The way to do that is look at what other kinds of research results are out there and are those similar and also do experts visibility review-- and we would have expected to see this, and do our expectations kind of sound-- and did we see errors that we expected? And do they also kind of look like what-- that the general public would kind of expect to see also, and that they hear about, and we did see that. So the question is were the differences statistically significant for the errors? And for the-- and they were for-- for these kinds of errors that we expected. Time on task did not show statistical significance. Could be for several reasons. Because the machines were very similar. If we got some radically different kinds of limitations, we might see statistical significant. We're not terribly concerned about that because we expect to see a lot more variability, and it may be the case with more users, you are still going to see such variability that you can't show significant staticly significant differences. Time on task also depends a lot on-- you know, the individual circumstances and the users, et cetera. We all-- dan, did you have a question?

Just curious since you went in to that. People when they are unfamiliar with something the first time they may have more errors, and sometimes when they get more familiar with that particular device, they adapt to it and do better, so--

Number of errors-- kinds of numbers of errors are similar to what we're seeing in the research nature--

You didn't try competitive used to come back and try again?

Was there between or in between participants.

Between.

Each participant only voted on one of the systems.

That's correct.

If I voted on a system i'm familiar with I might do better than a system I auz unfamiliar with, but if I went back to that system that I was unfamiliar with a time or two, which might happen you might have difficulty the first election but after competitive elections you might do just as well.

Most of our users didn't have a huge amount of experience with these, and-- one was a dre one was optical scan. People know how to fill in bubbles they were very different.

I'm curious about the age range. You said 21 to 30 that's our poorest age range for voting, and you might see different types of errors for an older population--

You might see more errors with an older population.

That's what I mean, and that's the typical voter.

This is the protocol.

[indiscernible] age group only.

No, but it talks about the next stage. That's correct.

After 2 000 there was a lot of speculation about how many people you would need to be able to find a settle error, and the way this bat ballot was instructed were to test different types of conditions, like one race has a lot of candidates and they are asked to vote for someone low on the list, for example, so it's both a little frightening and a little encouraging with a small group of relatively unchallenged voters did well.

The purpose here to-- to be a broken record was to test the protocol not the machine. The fact we were able to do this with a small number of users of people that you expect would do well and you still measured the range of errors with this ballot supports the individualty validity of the test protocol. And most people had what are considered good scores, and they were confident that they voted correctly, and we don't see any significant differences between systems, but what we expected this to be the case that the draw-- the important benchmark here is of course did they cast their vote as they intended? If they take a little longer one way or the another. Some voters were happier than others that's not as critical. But our thinking of using time on task and using the scores is report them and put a lower bound that says if a system score is worst than this system has big problems and to use those benchmarks in that way. Okay. So there's lots of different ways to count errors for the effective benchmark. You could just say-- just the strict binary did they fill it out correctly in total or not? Did they-- and the second binary was did they cast it or not? And you could calculate sort of a success rate of number correct over total number of participants. That-- that tends to not vsh -- tends to have very lose confident in-- [indiscernible] so if we went with binary we would have to test a lot of users, but for our next experiencement we can calculate the errors any way we want. We're looking to look at these errors and pick what we think is the best way to count errors. You can count number for each contest, you could look at each possible entry the voter could make. And either they should have voted for this and they didn't, that's an error. Or they should not have voted for this candidate and they did, that's an error. You can count and weight different kinds of errors as more serious than others. You have look at the number of individuals making a particular kind of error. In general you count those number of errors and divide by the numbers of participants time their voting opportunity per participant.

Question?

Uh-huh .

Uh-huh.

Did you have [indiscernible] on this?

Yes, we did. We told them what to write in. For dreshg e, it would be typed in.

Sharon?

Yes. This is me-- my opinion here, but it seemed to me that one of the discussion points we might have is whether we want to create a benchmark for errors, or whether there might be three or four different metrics, for instance, herly failure to cast might be treated different limit or how many people have different kinds of errors, you might have a-- a few people might have loot of errors, and you might want to look at the distribution of errors across the races. They always occurred in two of the tasks in this ballot which would indicate-- and I started thinking about what are the kinds of usability errors that are about indicating-- [indiscernible] usability of-- system-- of-- system-- [indiscernible] three or four different aspects of errors and it has to uk seed the threshold in all of them, because any one of them could indicate a kind of problem, and I have on the this out to them and they sort of said awe.

You can't just say, okay, we ran this test--

No. No. No. But we might not have to choose between these benchmarks we might be able to say there are two or three that are more likely to indicate a type of problem, and we would want to see a successful passing of the threshold in all of those.

Question. To that point, whitney, are you talking about -- still talking about test protocol? So you are still just testing? You're not talking about the voting public?

Yes-- no, we-- this-- we are just talking about a test protocol, and I think we should say the same thing about this test protocol about any test protocol. We just had a discussion about accuracy and real word ballots. We're creating a be it of a bubble and saying this sex actually how we'll test. That will not map exactly to necessarily any voter or precinct, but it's a--

We hope it's a prediction-- it's lab test. We hope it does give you a prediction of performance out in the field.

Right.

And that's why--

A controlled expiercement.

What are the errors that occur in this test against different systems with appropriate-- [indiscernible] because that would be the one that I would be concerned about the most is the under votes. Because people don't realize how many under votes there r..

As I understand it part of the instructions for voting this ballot include instructions to under vote.

Retry to be as comprehensive as we could with the different tasks. Okay. All right. So we're currently running experiments to determine reliability. So test repeatability, can the test results be repeated with the same test administrators and the same kind of participant demographics? Can it be reproduced--

Whoever is on line could you please mute your phones because it's coming through the speaker. Unless you have a question, that would be great. Thank you very much.

-- with a mix of age range, and geographic region. We're probably going to use virginia, maryland dc the test participants across the country, but that actually gives you urban and suburban and rural areas. So that's actually does give us a wider-- much wider geographic area than for the validity tests. And we're going to do a series of tests to see if we do get repeatability or reproduciblety. Then we may need to repeat them with some adjustments, depending on the earlier results, and then we-- we'll also bring in a wider range of commercial systems because we got to figure out a good baseline, so from-- from the performance gathered from wider representative set rather than just the two, we'll have to calculate, sort of a baseline that most can reach, but that is not so low that it's trivial to reach that baseline. Now, let me point out that we are not talking about participants with disabilities here. These are people using not the accessible but the regular voting station, we're assuming that they are typically, but they are not designated as having particular I haves disabilities, because that-- one would hope that our baseline for errors would be similar in that we could still use that but we don't know what kind of variability, what our confident intervals are going to look like and what our rates are going to look like, and that's kind of the next stage of research for the future.

And more precisely if you are using the audio ballot, you are actually using a different system.

Yes, it's a different system. We certainly would expect the time to be long we are the audio ballot. Yeah. Any questions? Hopefully we'll get a baseline in there very soon.

What is the time scale.

We want to get something in to the version of the vvsg '07, and we hope to complete the experiment by the beginning of april-- it's tight. We're really pushing.

David wagner. I'm not a usability expert, but I think you and nist and hfp are do a phenomenal job here, and thank you.

Thank you very much. Okay. Next research steps. We heard this morning from da net ta that they are going to be putting out some guidance on ballot design. When that is finally accepted by the eac we hope there's to look at it and make sure-- look it over to see if there's something we can also reflect in the equipment standard, but we haven't seen it yet, so we don't know. We are currently doing some research on additional voting plain lake wage guidance, it may be just-- it may be more appropriate in any case to make it as a guidance document for suggestions to the vendor for wording that works better, and just-- just make it as-- as a good guidance. Similar for color. We have some color requirements, but there is research throughout that we need to collect up and say these color combinations will work this is based on best practice. We also

want to do a small analysis of looking at how and when to use icons and pictures appropriately, so we don't introduce bias, and so they are not a distraction. We're also going to try to be working on, again, some guidance documents, so we put in to the documentation volume requirement that talks about that the documentation should be usable, and so we thought about how do you write requirements for that, and we weren't sure how do that, but we said, there's a lot of technical communication experts that do this all the time, and one thing they do is write style guides that say this is a good way to make sure this documentation is easy to read and look at, so we said we could do a template that would be a test method for judging whether documentation is usable or not. And I already talked about generating accessibility performance benchmarks, but we're way off from that. And--

Sharon, thank you. I would like to throw in one of the issues that came up, and that commissioner davidson is a question of how and when the standard can be updated and given the time constraints i'm particularly concerned that we can add in accessibility benchmarks as they are developed and so that we don't either leave them out entirely or rush and create bad ones, because we're rushing. That's one where it would be the same test protocol, the same basic requirements but where the benchmark might not be done in time for july-- well won't be done in time for july might be a fairer statement. Whatever the we is-- as they just consider how this is updated this is one of the issues I would like to be kept in mind.

Bill jerry. On what kind of time scale do you think reasonable benchmarks might be defensible? Is it august as opposed to july, or it's august, but of 2011?

I think that depends in part on this procurement .

We may have some influence on that.

Yeah. I'm thinking '08. Not--

Early '08.

Early '08.

This is patrick. I'm not sure if my question ties in to the testing as much more as the experience from ongoing voting activities especially with dres and how that experience is playing in to the development of the vvsg 2007. And I was specifically intriged with the report that came out last month. I think david was part of that report on the sar sewta, and it seemed to indicate it was ant system issue but more how the ballot was actually set up and the fact there's now lawsuits and potential bills in congress so forth. Is there something that is already in or will be put in to the vvsg that provides guidelines that to conduct an election means you lay it out, right?

It does appear there was a usability problem. There was a report also that suggested that. And as I said there is ballot design guidance coming from the eac that may help, but I haven't seen it yet, so I can't speak to that-- that's not in this work. We do have things like-- you know, consistency-- consistent wording in there now, and--

We're--

[indiscernible].

The ballot design, we have a meeting in kansas city. That is the main purpose for that public hearing that will be april 18th so that will be out at that time, so that-- I mean that will be coming very shortly after that time frame. But I do have a concern with your moving target. What you are doing is creating for manufactures a continued change in standards and guidelines, and that is what we're trying to get away from, because that's where our cost comes in. Every time you change something for the manufactures, if we have a july date, and then we come back and we have an august date, or we have a next year date, early '08, you don't-- I don't know how they can meet that.

Uh-huh.

And that just pushes-- that's my opinion, not the [indiscernible] but donanyta's.

Yeah. I think there will be continued research and that's an issue we have got to think about. Let's see the others--

Just to go back to the specific issue we're talking about. I don't see why there should be separate error and accuracy benchmarks for anybody using the system. So one solution-- a quite simple one is say one we have determined an acceptable benchmark it doesn't matter where you are testing the paper ballot or the audio ballot of a system, and that in fact the time might be different because-- and-- and how-- because if you are reading along, if a ballot has a long referendum on it, that takes longer to readout loud or if someone can listen with the tempo learned up that can takeless time. The accuracy and error-related benchmarks should be the same across the board, no matter how you vote. We might be able to solve this quite easelly that way.

We need to do a little experimentation--

But let me also point out that-- the benefit of having a performance benchmark with a test protocol is the vendors can run this themselves once we put all of the data out. They can run this they can use the same protocol for any reporting they do, and also at the state level, back to the ballot-- the florida ballot question, they can certainly use that test protocol with one of their own ballots, just to sort of see what kind of errors are they getting?

The other dhing that-- the example you brought up, but one of the election officials beats me to it is that narrow line between what the ballot layout capabilities of the equipment and actually laying out the ballot. Because there is human variation in that it's one of the reasons we asked the vendors to lay out the-- I know this project has been going on-- I have been waiting with baited breath to hear the results because I think the group doing it is interesting, creating layout guidance for the election officials to use, one of the things we want to use is look at that now that we know it's april 18th, we want to look back at it and say are there things they are suggesting as good practice that we would add to or amend or make a requirement to make sure the systems support or encourage that.

When you talk about-- when you tested-- just two different types of devices. And then vendors design it any way they want. If i'm benchmarking two dres or two optical scans it could be one vendor was better at playing out the design and the equipment is no no better.

But somebody has to lay out that ballot.

But wouldn't you want something that is more representative of what the designs are coming out of the field.

Well--

[indiscernible.]

Or would you want to be able to get output from these results that might give you feedback on-- on better ways to do a ballot design?

That's something that the skren dors might get out of seeing any results of, but it's not the purpose of the test. And I think we need to be careful between distinguishing between an evaluation that tests the performance of the system under certain circumstances and design guidance back to the vendor.

Let me put it a different way. Suppose you did a test. We had the same piece of equipment and you handled two different designs and you found you had more variability in the test results that way than from the equipment themselves?

I wouldn't be--

Which might be the case.

I wouldn't be particularly surprised by that result. There's certainly easy to do bad designs and it's hard to do good designs, but we're not testing the ballot design capability of election officials, although we're trying to encourage systems that provide good designs. There are aspects of the system that can't be changed by the election official, and we want to make sure that those put them in a situation where they can't design a good ballot, and I think that's-- it is a-- it is a very difficult area to separate which is which. And I think that-- I have been very impressed with the process that you have gone through and make sure the test itself is not inducing any more bias than any test inevitably produces?

Ron?

David compliments on the group. It looks great. It seems when you introduce the general adjustablety, you introduce some hazards with the voter turning off the audio or changing languages to a language it can't read. I don't know if it's a requirement-- so I just wanted to inquire--

There's a reset back to-- it's in '05. .

So that does include-- so any voter at anytime can reset to a standard state. Is that the requirement?

Yes.

And furthermore than the machine resets to a-- so a voter doesn't come in and find it being set for a previous voter.

Okay. Thank.

I-- sort of a comment to the group. I would actually like to follow-up on commissioner davidson's comment. You know, i'm not sure-- i-- I agree with your sentiments and I think it would be difficult for us to put out next iteration guidelines and start going through standards boards and public comment and

others with-- [indiscernible] in there, and if there are possibilities with simply coming up with a consistent way of looking at it, and that was a somewhat intuitive concept you proposed. I think what the testing would do at the end could be used to validate the assumptions, and if there's an agree gous error that arises in that it may be easier to correct the egregious error than having to go through the process again entirely.

That's a good point. I know from being-- [indiscernible] procurement and arrangement the mechanics can be a challenge, so I turn to you as the head of nist to do anything you can to help smooth that process.

I'm formally task my staff to talk to me immediately after this about whatever issues there may be on that.

I have a question they would like to ask. I didn't see anything in the presentation on a-- usability on paper ballots. And the-- where it comes from is in the soft-- I mean in the software independence resolution there was a requirement for paper-based machine, and, you know, I seem to think that we need some type of a study to go along with that--

I'm trying to understand your question. The optic scan in this validity was--

Paper records.

Right.

Paper trail the ability to accurately verify those you mean?

Just a study on the usability of paper, I think is real important. And I just didn't see that and I wasn't sure if it had been discussed or not.

A couple of ways to look at it one is if the usability encompasses any system that might be tested that include [indiscernible] paper ballots-- that's one answer. I can't see you past the podium, and I don't know if that's the question you were trying to ask.

I just-- you know, I just didn't see that type of a setting already done to see how people react to the paper, you know, and that was one of my concerns and I don't know if there there is any--

No specifically looking at what happens when a voter is confronted with a paper audit trail? I don't think we have anything like that on the schedule.

David wagner, it seems to me if I understood correctly what you are trying to accomplish is to design a protocol that you could use in testing confirmablety of any system. It seems like that isn't the scope of the tgdc to do new research on-- on how to design the best [indiscernible] pad or something like that necessarily.

When they are having as many difficulties in counting that paper.

Oh. Oh. Okay.

Usability for election officials?

Right. The election officials are complaining that this is very difficult, and, you know, whether we-- you know, I know there's been some discussion about bar

codes, whether they should be used or should not be used, but I tell you, what they do it by hand it's a disaster.

I think the issue for me in trying to design what would the study be. We know there's difficulties in hand counting paper. Data already tells us that. There are different ways to help with that so-- so I have had trouble formulating what does it--

I probably should come to a mike, but there are certain things that the manufactures are doing right now. Some are using a bar code. Is that successful? I mean there's some studies there that maybe would create a differences of-- in the minds of the tgdc members, if there is something that would be more successful than obviously hand counting that ballot. What kind of ability can they scan it or whatever? But there is things out there right now, and so I just wondered if that was being thought of.

I think that-- that is something we're going to discuss--

I think alan needs to identify who was talking--

David--

Earlier was whitney and done natta davidson.

I don't think if that's something we want to discuss tomorrow on ways to improve it and research and so forth, so if you want to hold that thought-- and if don't address it all then make sure we change what we're talking about to address those issues, but I think that is addressed. Wouldn't you agree, john, that we're starting to border on that a little be it?

Ron?

I think that's a great issue the usability of the audit -- the audit is very important so being able to make sure that's usable for the poll workers is very important. Bar codes is something we have discussed a lot. And it's something that the voter can't check himself and you have a real issue in terms of verifying the bar code-- but there are approaches to working with bar codes and human readable to. Lots of interesting approaches, and I agree that's a great area for research and further improvement. I'm not sure how much can put in to the standards in terms of the time we have got here.

Whitney.

Sorry, just . . .

So if I can add to what ron said let's take it to the plea for input and suggestions and further comments on this issue, because I think it is a critical one.

Yeah, I think-- one of the things that are a real challenge for those of us who are not election officials, it's easy for us to imagine the usability challenges in voting, because we are voters, and because that task is fairly well documented and well understand. What you guys do is at least a magical art, and so help in understanding how to formulate a question that could be answered, you know, what is it-- do we want to do time tests of different-- of different types of audits?

What has been helpful to me-- is there some requirement that would go one way or the another that we could do some research that would inform us and tell us what that requirement is.

I think we all understand the general problem but not how to get down to something specific enough that we can charge somebody with doing the research.

Helen. Main thing is we don't make though errors we have made in the past. We were given certain things we had to accomplish by the 2006 election, both the election officials and in particular the manufacturers were given very little time to do that. We were given dres and in some waits we were required to have [indiscernible] pats, and with that we had things added to a dre that gave us a big printer that had tape in it that a lot of people couldn't handle, couldn't be changed, so if we don't get in to a scenario of going back to the same thing of giving us something else in a short period of time that we have to do and the manufacturers have to provide us-- you know, anything we can do to avoid that.

One thing I would point out is that one of the things in here, in the vvsg '05, we had requirements for usability test reports presented by the vendor for the general usability and then three groups of-- of testing the different interfaces for people with disabilities. We have added one in this, which is testing with [indiscernible] workers so we would actually be doing usability tests with set up and observation, of of the things we have heard would come out in that test. It's not a test of the audit, but it is certainly a test of the-- during election maintenance-type, and operations stuff so we have gotten that piece in. How we get to the next phase, which is the audit is the one that I find a challenge.

Always get concerned when we start talk about what I'll call the third rail for the election administrators, and that's when we start writing standards for them in terms of poll worker conduct, and poll worker training. I think that's not our jurisdiction.

Yeah.

Uh-huh.

Absolutely. I was thinking more of things like can you follow the instructions to open the thing-- can someone given a set of instructions can they follow the steps? And those are manufacturer's instructions.

If I could respond a little fwoit secretary gail, the intent is not to come up with any requirements for audits or for how they ought to be conducted. The intent, really, is to look at the paper itself that gets produced in vp pad systems or op-scan or whatever, or what can be done to that painer or to the format of it or to the format of beginning of day end of day reports so that it's easier for poll workers to handle, and so it's easier for election officials to use it, but no requirements for how they should be used, it's just-- basically, make it easier to use.

Okay. Are there any other comments, questions? Okay. Sharon, did you get the information that you need out of this session to continue to move forward?

Yes, I have.

Okay. If there are no other questions or comments, do I hear a motion to adopt the preliminary draft human factors and privacy section consistent with the

discussion we have had. A motion and a second. If there are any on any objection?

This passes by unanimous consent. And that, actually ends today's discussion. Almost an hour early, so thank you. For those of you who have to catch the bus, you should have-- to the metro, you'll have no problems. For the rest of you we reconvene to tomorrow morning at 8:30-- okay. 8-- 8-- so at 8:30 back in the same room.

You can leave your stuff here. It will be locked up.

Okay. Again thank you very much. I would like to thank the eac commissioners for providing valuable input. Meeting is adjourned for today