Meeting Minutes (Official)
Technical Guidelines Development Committee (TGDC) Meeting
December 4-5, 2006
National Institute of Standards and Technology (NIST)
Gaithersburg, MD 20899

Members in Attendance:

Dr. William Jeffrey – Chair
H. Stephen Berger
Patrick Gannon
Tricia Mason
Alice Miller
Philip G. Pearce
Helen Purcell
Whitney Quesenbery
Ronald Rivest
Daniel Schutzer
Sharon Turner-Buie (via Conference Call)
David Wagner
Britt Williams

Committee Support Staff:

Phil Greene, General Counsel Office, Department of Commerce
Mark Skall, Chief, Software Diagnostics and Conformance Testing, Information Technology Laboratory (ITL), NIST
Barbara Guttman, Software Diagnostics and Conformance Testing, ITL, NIST
John Wack, Software Diagnostics and Conformance Testing, ITL, NIST
Alan Goldfine, Software Diagnostics and Conformance Testing, ITL, NIST
David Flater, Software Diagnostics and Conformance Testing, ITL, NIST
Wendy Havens, Software Diagnostics and Conformance Testing, ITL, NIST
Lucy Salah, Software Diagnostics and Conformance Testing, ITL, NIST
Allan Eustis, Software Diagnostics and Conformance Testing, ITL, NIST
Lynne Rosenthal, Software Diagnostics and Conformance Testing, ITL, NIST
Sharon Laskowski, Information Access, ITL, NIST
John Cugini, Information Access, ITL, NIST
Nelson Hastings, Computer Security, ITL, NIST
Curt Barker, Computer Security, ITL, NIST

December 4, 2006: Morning Session # 1

Dr. William Jeffrey, TGDC Chair, called the seventh plenary session of the Technical Guidelines Development Committee to order at 9:00 a.m. He introduced himself as the Director of the National Institute of Standards and Technology (NIST) and Chair of the Technical Guidelines Development Committee.

After the Pledge of Allegiance, the Chair recognized Mr. Phil Greene as the TGDC Parliamentarian and requested that he determine if a quorum of the Committee was present. Mr. Greene then called the roll (see Table 1). Fourteen TGDC members answered “present.” Mr. Greene notified the Chair that a quorum (simple majority) of the Committee was present either in person or via conference call connection. (Note: Mr. Pearce arrived five minutes after the initial roll call.)

Dr. Jeffrey thanked the Parliamentarian. He then introduced newly confirmed Committee members. “I am pleased to welcome four new members to the TGDC: Ms. Tricia Mason and Mr. Philip Pearce representing the U.S. Access Board, Dr. David Wagner representing the American National Standards Institute, and Mr. Paul Miller representing the National Association of State Election Directors.” The Chair offered each of the members the floor for introductory remarks.

Ms. Mason thanked the Chair and commented that she looked forward to representing the U.S. Access Board. “I look forward to working with this Committee as well as the Election Assistance Commission’s Board of Advisors.”

Dr. Wagner remarked on his representation of the American National Standards Institute (ANSI). “I should mention up front that, consistent with ANSI’s policies, I will be abstaining on all votes. I am looking forward to working with the TGDC. Please do not take the abstentions as a rejection or endorsement of anything that folks are saying here. I just wanted to get that on the table for starters. Thank you again.”

Mr. Miller noted that he will be representing the National Association of State Election Directors (NASED) - the organization that began the voting standards development process. “I am filling the shoes of Paul Craft who has been part of this process from the very beginning. They are huge shoes to fill, but I am looking forward to the challenge. Thank you.”

Mr. Pearce expressed his appreciation for the opportunity to work with the TGDC. “I have tried to bring myself up to date, and one of the things that I have found is that you have written a lot of material and it is good stuff. I appreciate the hard work that you have done, and I look forward to getting a chance to work with you to, hopefully, provide some insight from my perspective. So, thank you.”

Dr. Jeffrey offered other Committee members the opportunity for initial remarks. He recognized Mr. Berger.

Mr. Berger noted that three draft resolutions were circulated among the TGDC in the last week. He offered introductory remarks on the intent of these resolutions that would be offered for discussion later in the meeting. “The three resolutions basically look to ensure that our efforts are as directly linked to the problems we are seeing in the field as possible. The first one primarily looks at the issue of the causal factors that created the system as we have it today, assuming that that system was created with good intent and for rational reasons. Basically, the resolution asks what are the trade-offs? The second resolution asks for a survey of the recent experience in the last two elections and a mapping of what the TGDC is doing to issues that have arisen in the field. The third resolution asks a fairly simple question but an important one: What problems are best solved by revisions to the standard as opposed to changes at other points in the system? (Text of all resolutions passed at this plenary meeting is available at: http://vote.nist.gov/AdoptedResolutions12040506.pdf. Text of resolutions voted down by the Committee is available at: http://vote.nist.gov/failedres12040506TGDC.pdf.)

Hearing no further requests, the Chair noted that Nebraska Secretary of State John Gale and Ms. Sharon Turner-Buie were unable to attend this meeting due to their current responsibilities related to certifying the November 2006 election results. He indicated that they would join the meeting via teleconference as their schedules permitted.

The Chair acknowledged the public service commitment of departing TGDC members Dr. J.R. Harding, Mr. Jim Elekes, Mr. David Karmol, and Mr. Paul Craft. “We are a lot better off for the contributions that they have made.”

Dr. Jeffrey recognized a motion to adopt the December 4-5, 2006, TGDC meeting agenda. The motion was seconded. The motion to adopt passed by unanimous consent. (The TGDC meeting agenda as adopted is available at: http://vote.nist.gov/TGDCagenda120406.htm.)

The Chair entertained a motion to adopt the March 29, 2006, meeting minutes. A motion was made and seconded. The meeting minutes were adopted by unanimous consent. (The official meeting minutes are available at: http://vote.nist.gov/Plenary032906-Minutes.pdf.)

Dr. Jeffery provided a brief history of the work of the Committee for those new to the process. “As a brief review for the public in attendance and viewing the web cast, Public Law 107-252, the Help America Vote Act (HAVA), establishes the Technical Guidelines Development Committee. HAVA charters the members of this Committee to assist the Election Assistance Commission with the development of voluntary voting system guidelines. Since the last meeting of the TGDC, three working subcommittees have continued drafting and editing preliminary reports on issues pertinent to voluntary voting standard recommendations in the areas of human factors and privacy, security and transparency, and core requirements and testing of voting systems. We will be discussing these reports today.”

The Chair then clarified the role of NIST and preliminary reports that are drafted for Committee review. “The recent news reports regarding the vulnerabilities of electronic voting systems contained in one of the reports to be discussed today have raised the question of whether the report’s recommendations represent the official position of NIST. This draft report was prepared by staff at NIST working with the Security and Transparency Subcommittee at the request of the TGDC specifically to serve as a point of discussion at today’s meeting. The report is a discussion draft and does not represent a consensus view or recommendation from either NIST or the TGDC. The TGDC, after discussion today, may adopt, reject, or modify the recommendations. Those reports adopted by the TGDC will be developed into guidelines that will be presented to the Election Assistance Commission for consideration. Any draft guidelines approved by the EAC will undergo stringent review, including public comment, before they are issued as final guidelines."

Dr. Jeffrey noted that the time required accomplishing the agenda items meant that the Committee cannot take public comment at this meeting. However, there will continue to be opportunities for the public to comment on relevant issues. "Comments and position statements regarding the work of this Committee should be sent to voting@nist.gov where they will be posted on the voting website. Comments we have received to date have been posted and reviewed by NIST staff and TGDC committee members."

The Chair then recognized US. Election Assistance Commissioner Donetta Davidson and offered her the floor for remarks to the Committee.

Commissioner Davidson thanked Dr. Jeffrey and the TGDC for their hard work. "Today, we are discussing future voting systems to make sure that the guidelines keep up with the pace of technology and, at the same time, are secure, accurate, and reliable. That is a tall order, but I am sure that we- the TGDC and the EAC- can all accomplish this as we work through the process." The Commissioner then reviewed an implementation timeline for the current voluntary voting system guidelines (VVSG2005) and the next iteration guidelines (see: http://vote.nist.gov/Davidson.pdf). She noted that the EAC testing and certification program would begin January 1, 2007. All voting systems would be required to be tested to the VVSG2005 after December 13, 2007. With required public comment and review, the EAC would not likely adopt the next iteration of the VVSG before spring of 2008, assuming a delivery of recommendations from the TGDC in July 2007.

The Commissioner asked the Committee to reflect on various options and implications on the election community. "Involved with elections as a former Secretary of State, I can tell you firsthand that one size does not fit all. We need to remember that each state has unique election laws. That means there are varying requirements from state to state. When we are looking at the new voting-related technology, we have to take into account the needs of all states. I believe that the voter verified paper audit trail (VVPAT) is only one option. We should continue to research other forms of verification because technology and alternate solutions in this area, I believe, will rapidly increase."

The Commissioner then posed future dilemmas for courts as the ultimate arbiters in VVPAT recounts. "Assume there is a recount that is held in a state with a VVPAT requirement because of a very close election, and resolution goes to the courts. Suppose that the VVPAT failed, because of improper loading or jamming. What is the court going to decide when the number of people that appeared at that polling place is different than the recorded number on the paper tape? Or, the voting machine has the correct number on it but the paper is missing. What is a judge going to decide? Are there two official ballots or is there one? Some of the states have said the paper is the official record, but is a court going to disenfranchise those people that showed up at the polling location to vote when their vote is not being counted because of a printer error? We really need to keep our doors open to technology. Any time we can improve the process in elections, we need to not close the doors to future solutions."

Commissioner Davidson also recognized the HAVA mandate to ensure that voters with disabilities can vote privately and independently. "I believe that we have to consider their rights as we move forward."

The Commissioner remarked that 2006 had been an eventful year for state and local election officials, especially with HAVA deadlines and new voting equipment. "We had over 30 percent of our voters voting on new equipment this last election. Election Day went a lot smoother than people anticipated it would. According to the public and the media reports, we have over 6,700 jurisdictions that ran elections and only 39 reported problems. That is less than one percent. Most of our voting officials had contingency plans in place including extra paper ballots and backup batteries. They extended polling hours in some places as needed. Election officials, poll workers, and voters successfully met the challenge of Election Day 2006. The exit polls that were done by CNN indicated that 88 percent of the voters were confident that their votes were counted accurately and that the election was handled securely."

Finally, Commissioner Davidson again expressed her appreciation to the members of the TGDC. She remarked that this meeting of the TGDC may be the most important plenary held so far, as it will address new guidelines for future voting systems. "The manufacturers have to have time to develop new systems, and the EAC has to have time to implement new guidelines. That's why I really focused the time frame. As the TGDC moves forward, obviously I hope you consider time frames as well."

Dr. Jeffrey thanked Commissioner Davidson. He then asked Mr. Mark Skall, chief of the NIST Information Technology Laboratory's Software Diagnostics and Conformance Testing Division, to review the activities of his team since the March 2006 TGDC plenary.

Mr. Skall thanked the Chair and began a review of key events since the March 2006 TGDC meeting. They included:

- Continued development of VVSG 2007
- Improved access and coordination with the TGDC
- Other coordination and research
- Interactions with Congress.

Mr. Skall highlighted the standards development research development by NIST scientists in coordination with the three TGDC working subgroups including:

- Human Factors and Privacy (HFP)
    - o Usability performance benchmarks and updates to usability requirements
    - o Updates to accessibility requirements

  - o Other areas: alternative languages, documentation, plain language, and timing

- Core Requirements and Testing (CRT)
  - o Commercial off the Shelf (COTS) and testing issues
  - o Mean Time between Failure (MTBF), reliability, accuracy
  - o Coding conventions
  - o Quality issues

- Security and Transparency (STS)
  - o Software Independence and DRE security issues
  - o Software IV and End-to-end cryptographic systems
  - o Voter-verified paper records issues and requirements
  - o Wireless
  - o Setup validation
  - o Other core security areas: access control, audit, crypto, physical, setup validation.

He then summarized specific coordination efforts between NIST and the TGDC including monthly "builds" of drafts for sections of the VVSG2007. Mr. Skall also highlighted the frequent communication between NIST and the EAC as well as outreach efforts to the election community. "In the first version, VVSG 2005, we were constrained by the nine-month time limit given to us by HAVA. We did not have as much time to go out and speak to as many people as we would like. One of the things that we have really tried to do for this particular version of the guidelines (VVSG 2007) is to do a lot more outreach." He provided examples of the outreach, including interactions with Congress:

- Monthly meetings with EAC
- Monthly meetings with vendors via the Information Technology Assoc. of America
- Liaison with EAC's Standards Board & Board of Advisors
- Meetings and coordination with other researchers
- Briefings at conferences, e.g., NASS/NASED
- Informational visits with election officials
- Observing and volunteering at elections
- Testimony of Dr. William Jeffrey before the House of Representatives Committee on House Administration and Committee on Science
- Presentation to a Voting Town Meeting hosted by Congresswoman Millender-McDonald.

Mr. Skall concluded with a review of the agenda for the plenary meeting. He discussed the strategy for the NIST presentations. "We are going to give high-level summaries on most of the material and spend the majority of our time on the key issues. We want to spend time debating the issues that Committee members feel strongly about."

(Mr. Skall's full presentation is available for review at: http://vote.nist.gov/Voting-Activities-Update-Skall.pdf.)

The Chair thanked Mr. Skall and called on Mr. John Wack of NIST's Information Technology Laboratory to present an overview of the proposed VVSG 2007 document structure.

Mr. Wack thanked Dr. Jeffrey. He briefly described the challenges inherent in producing this document. "The first thing I want to get across is that we have two jobs here at NIST, and one is to write requirements. And we have to do a lot of research in order to come up with good requirements. The second thing, which is almost equally as difficult, is to put together a document in such a way that it is understandable. We have come to recognize that not only is the quality of the requirements important, but also the usefulness of the document to the customers. So, we have a difficult job because we really have to write for voting system vendors, test labs and states. Basically they all have to be able to find requirements they need, interpret them unambiguously, and make decisions based on them.

With regard to format and usability of the VVSG 2007, Mr. Wack noted the following intentions:

- A goal of facilitating TGDC review of the document by providing draft material in an assembled document structure
- A goal of delivering to the EAC a readable, well-formatted, highly usable VVSG
- A focus on simplicity, plain language, a 'flattened' structure, and easy-to-navigate tables of requirements
- Coordination with the EAC as we go along to ensure we understand formatting and relevant policy issues.

Mr. Wack reviewed the proposed VVSG 2007 document structure:

- Volume 1: Introduction
- Volume 2: Glossary, Definitions, Terms
- Volume 3: Product Requirements
- Volume 4: Vendor, Test Lab Data and Document Requirements
- Volume 5: Test Methods

Mr. Wack indicated that the VVSG2007 volumes are under active development, and NIST staff was hopeful of decisions by the Committee at this meeting to further define directions and approaches to assist with completing the draft VVSG2007. He noted that only seven months were left to complete the guidelines including final review and approval by the TGDC.

In conclusion, he explained that the VVSG 2007 would undergo a review by the election community in a manner similar to the review of the VVSG 2005. "This document has to go out for a public review. There will be many different audiences judging it at that point. So, we recognize that the better job we do getting across our material, the better job the Committee can do in judging it and the better job the public can do in assessing it."

(Mr. Wack's entire presentation is available for review at: http://vote.nist.gov/VVSG-2007-Overview-Wack.pdf.)

The Chair then asked Mr. Curt Barker, Chief of NIST's Information Technology Laboratory's Computer Security Division, to introduce the Preliminary Reports of the Security and Transparency Subcommittee.

Mr. Barker thanked Dr. Jeffrey. He initially stated the high-level overriding considerations for assuring trust and confidence in elections by the public including the independent verifiability of election integrity. "Our goals are to provide process integrity and maintain the accuracy of results in the voting system, and, as importantly, maintain public confidence in the process, integrity, and accuracy of those results."

He briefly reviewed some of the security mechanisms under review for assuring the integrity of the voting process including cryptographic and non-cryptographic verification protocols.

In conclusion, Mr. Barker noted that the Preliminary Reports to be presented today would address:

- The concept of software independent verification (IV)
- The restructuring security components for VVSG 2007
- An Update on VVSG 2007 security requirements.

(Mr. Barker's full presentation is available at: http://vote.nist.gov/STS-Intro-presentation.pdf.)

Dr. Jeffrey thanked Mr. Barker and asked Mr. Wack to summarize the STS recommendations for the Committee.

Mr. Wack thanked the Chair. He reported that the subcommittee recommendations will deal with ballot auditing capabilities for future voting systems. He indicated that Professor Rivest would follow with a presentation on the concept of software independence. "He will also discuss recommendations for encouraging some new and innovative approaches that promise greater usability, accessibility, and reliability in voting systems."

Mr. Wack provided an overview of and rationale for independent audits of electronic cast ballot records and independent verification. He noted that the STS Subcommittee had reached an initial conclusion. The conclusion is that VVSG 2007 should require future voting systems to produce records of ballot choices that can be readily and independently audited.

Mr. Wack offered rationales for the auditability requirement including:

- Voting systems are computers that are by nature buggy and difficult to secure.
- The absence of an independent audit capability in DREs requires reliance on getting the software 'right' and keeping it that way.
- With an (A) independent audit capability and (B) by performing routine audits, bugs and security problems will be easier to detect.
- An independent audit capability is preferable for security-critical environments.
- Building in an audit capability from the ground up helps to assure that the software is indeed correct.

He then addressed the auditing capability of the direct record electronic voting systems now in use. "The direct record electronic or DRE voting system can be audited to a certain extent. You can check how many records it has recorded, but it is insufficient overall for detecting whether the ballot was recorded as cast by the voter. So the approach taken by the DRE requires relying on the correctness of its software to record the votes correctly."

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

Finally, Mr. Wack concluded with VVSG 2007 security recommendations for the full Committee to consider for future voting systems. Specifically, the STS Subcommittee recommends that guidelines:

- Include only approaches that are independently auditable
  - This means, for VVSG 2007, Voter Verifiable Paper Record Systems
- Include improvements to paper-based systems such as:
  - Improved usability and accessibility
  - Better reliability
  - Easier auditability
- Encourage development of new, secure, possibly paperless approaches that could result in systems that are more usable, accessible, and easier to audit.

(Mr. Wack's entire presentation is available at: http://vote.nist.gov/STS-Auditing-Recommendations-Wack.pdf.)

The Chair adjourned the meeting for a fifteen-minute break.

December 4, 2006: Morning Session # 2

Dr. Jeffrey called the plenary meeting back to order. He then called on Dr. Rivest to begin an overview and discussion of software independence (SI) and encouraging innovation in the VVSG 2007.

Dr. Rivest thanked the Chair. He also thanked Commissioner Davidson for her earlier remarks encouraging innovation. He then highlighted two STS subcommittee recommendations:

- "Software Independence" as a requirement for voting systems in VVSG 2007
    - recommends NIST focus on current SI VVPR systems
- A process for considering new SI approaches such as end-to-end, and new, innovative, possibly paperless SI approaches be encouraged in VVSG 2007 for future voting systems

"I want to describe software independence to you and say what it means. We will have a resolution talking about that and recommending that all voting systems be software-independent in the future. The second recommendation encourages innovation basically saying that we do not know enough about how to build voting systems. We really need to encourage more innovation."

Dr. Rivest then described features of software-based voting systems:

- Software is, on the one hand, wonderful: it enables the design of rich, flexible, and powerful systems and of adaptable interfaces for voter.
- On the other hand: all software is buggy (typically 4-5 bugs per 1000 lines of code).
- From a practical point of view, it is impossible to write bug-free code for a large system.
- A voting system is software-dependent (SD) if an undetected bug in or modification to its software can cause an undetectable change in the election outcome (i.e., not detectable even in post-election audit or recount).
- A voting system is software-independent (SI) if it is not software-dependent.

Dr. Rivest explained his view that the software is the key problem from a security vantage point. "If an undetected bug, a bug that wasn't detected during the development process or in testing, or a modification to the code can cause an undetectable change in the election outcome, that is sort of the worst possible result from a voting point of view. You have an election result that is wrong, and you have no evidence to show you that it is wrong. There is no audit or post-election test you could do that tells you if you have the wrong result. That is a software-dependent voting system."

Although the terms "software dependence" and "independent verification" are close in meaning, Dr. Rivest suggested that "software dependence" is a more useful term than the term “independent verification” used in the VVSG 2005. “Use of SI terminology emphasizes the most significant problem: relying on the correctness of software for the correctness of election results.”

Dr. Rivest noted that “software” also applies to firmware and hard-coded logic, both of which are software-based. He then reviewed his concerns with allowing software dependence in future voting systems including:

- Future voting systems will continue to grow larger and more complex.
- Assuring that complex software is correct is, for all practical purposes, impossible.
- Software is difficult and expensive to test to high degrees of confidence; typically only doable for very small systems.
- Voting system software would need to be stripped down and this would be very costly, yet correctness would undoubtedly still be questioned.

He then provided an overview of the following topics:

- Requiring SI in VVSG 2007
- Future SI approaches
- Ramifications of SI
- Security of existing DREs
- Implications of not requiring SI in future voting systems
- Classification of voting systems as SI or SD.

Mr. Berger asked Dr. Rivest to describe the relevant threat model on which SI is based.

Dr. Rivest noted that, in fact, the threat model is the starting point for analyzing security risks. “When we are talking about software-dependent systems, we are talking about threats to the software. They may be threats which are, in some sense, inadvertent. You have software dependence, so you have a threat of bad coding in the beginning. Also, you have the threat of insiders in the process somewhere producing bad coding, changing the software either at the vendor or somewhere along the distribution chain. When you have dependence on the software, the threat model is any threat to the integrity of that software in terms of either its design or its delivery. ”

Mr. Berger asked Dr. Rivest if he proposes to maximize subsystem security with SI as opposed to security of the whole voting system.

Dr. Rivest replied that the goal is to maximize the verifiability of particular election results. “It is not the question of evaluating the security of the system so much as verifying election results. You would like to have confidence in each and every election result.”

Mr. Berger asked whether software independence forces reliance on other parts of the voting system. “What are those dependencies and what has happened to the total security of the system? Have we perhaps become less secure because we are now more dependent on an even less reliable component in the system, for example, human error?"

Dr. Rivest noted that adding security checks to the voting system typically allows one to detect additional vulnerabilities. Subtracting checks does the opposite. "So you could take a DRE plus VVPAT and throw away the VVPAT. Now, you have a voting system which checks less frequently and therefore is more vulnerable. You are talking about security here and taking away checks never helps."

Mr. Pearce asked Dr. Rivest if the STS subcommittee had considered the impact on state and local election officials of requiring SI voting systems.

Dr. Rivest replied that, definitely, there were transition and timing issues here. He felt that Commissioner Davidson might better speak to these from a policy vantage. "As you change requirements over time, states need to adapt. Transition planning and costs would be incurred. The changes need to be scheduled appropriately. However, there is certainly no dramatic instant changeover that needs to happen. I think with all due deliberation and accounting for normal budgets cycles, these things can be accommodated."

Dr. Wagner, a member of the STS subcommittee, elaborated on this matter. He noted that the SI requirements would apply only to future voting systems. "So, the SI requirement for voting systems would not affect the use of existing systems. That is, the jurisdictions would be able to continue to use existing systems. The place where this requirement has an impact is in the future with voting equipment submitted for certification after 2010. Then this SI requirement would place the restriction that if a state or local jurisdiction wanted to buy new voting systems, then those new systems would need to be software-independent."

Dr. Schutzer expressed somewhat of a disagreement with Dr. Rivest's premise. "If I put myself in the shoes of a state that had invested in a DRE machine without a verified voter paper trail, I now see I have two years to act. If I agree with the conclusion, that SD systems are somewhat vulnerable, it would be incumbent upon me to look for a field upgradeable fix to the DRE machine, which would mean some way of retrofitting it with a printer, for example. I think I might well consider doing that using available technology today. I do not think there is anything wrong with that. But I think that it would be advantageous to consider that plan of action."

Dr. Schutzer also advised the Committee to consider the interdependency and interaction of voting machines with all other parts of the voting process. "Number one, you find that it is a cause of a lot of the security concerns that we are seeing in current elections. This Committee might also find some ways out of the dilemma of how you arrive at independent testing of voting systems. So I would say I do think an SI requirement would create an immediate impact if I was an election official."

Dr. Rivest agreed that there could well be some impact.

The Chair offered a reminder to the Committee of its role under HAVA to provide just the technical guidelines for voting systems. “The time scale for the implementation of the guidelines is under the purview of the Election Assistance Commission. In other words, the decisions as to how the guidelines we produce may be rolled out in the future are within the scope of the EAC with the guidance and input through their public hearings. I don’t think that, as part of the development of the guidelines, that the TGDC would be providing specific rollout strategy.”

Dr. Williams commented on “absolute” assumptions of the STS subcommittee with respect to the complexity of software and testing it for bugs. “We do not live in an absolute world. We live in a probabilistic world. The correct question is this: Can you test the software to an acceptable level of security? The banking industry is an illustration of the fact that the answer to that is yes. They move billions of dollars around every day with this buggy software without ever producing a single piece of paper.”

Dr. Schutzer emphasized a significant difference between banking and voting records. “With all our software, the banking industry retains the identity of the individual and the parties to that transaction. We do not have this additional problem of the secret ballot. So, therefore, I can go back when the verified software issues crop up as they do in online banking. I can trace back the transaction issue to the individual party.”

Dr. Williams suggested discussing the trade-off between secret ballots versus voter verifiable ballots.

Mr. Berger suggested further discussion of software independence within the context of Dr. Williams and Dr. Schutzer’s previous remarks. “SI may not be the best construct to work in. There is the context of general computing and general computing software. There are other heritages of software, control systems, security systems, and instrumentation that are much more deterministic, much more reliable, and much more verifiable. Perhaps we should explore a stronger construct to talk about software independence or discuss moving voting equipment to a different software heritage where it is more verifiable.”

Dr. Schutzer clarified that he believed software independence was a good way to frame the issues. He provided the committee with a possible “armchair engineering” example of software independence where a future voter receives a unique transaction number so that only that voter can validate the vote before the vote is tallied.

Dr. Rivest thanked Dr. Schutzer for the example and noted that it would fit within the STS subcommittee’s proposed innovation class for voting systems. “These are new approaches which are not representative of what the industry is doing now, but which I think we ought to try to support through the innovation class here. So, the software independence restriction does not mean that these ideas are excluded, because I think you can also have those kinds of approaches explored. They are new approaches which need to be encouraged and vetted.”

Dr. Rivest concluded with an explanation of ways that the innovation class could be set up and new voting systems evaluated. He put on the table the possibility of Congress funding research grants.

Dr. Jeffrey noted that it would not be appropriate for this Committee to make a funding request to Congress. He then opened the floor for further discussion on Dr. Rivest's presentation. (Dr. Rivest's entire presentation is available at: http://vote.nist.gov/STS-SI-Rivest.pdf.)

Ms. Quesenbery offered the paradigm of "equivalent facilitation" that exists within Section 508 of the Federal Accessibility Requirements. "Those regulations acknowledge that when you write a requirement, you are frozen at a point in time, but that in the future, new technology might be developed that would enable a vendor to meet a requirement in a new way. It allows vendors to submit a statement of the accessibility of their product. In it they can say, well, we don't meet this requirement in exactly the way it is written, but we meet the spirit of it in a new way using new technology. So, there is already some experience within the regulatory world."

Mr. Berger supported Ms. Quesenbery's comments. He briefly recounted his understanding of "equivalent facilitation" as a member of the Section 508 advisory panel. "If a vendor can show that they meet the high-level intent in some way that does not specifically meet all the detailed specifications, then the product can be approved. So, I think if the TGDC were going to implement something similar to equivalent facilitation, we would need to make sure we have defined that high-level intent as the criteria that you get judged against."

Dr. Rivest noted that the starting point for framing high-level voting systems requirements would be in terms of integrity of the count and of voter privacy.

Mr. Berger commented that "equivalent facilitation" becomes a helpful determination of inadvertent flaws when they arise. "If something meets all the detailed requirements, but clearly fails the intent because it is not secure or is not accurate, you can go up to the high-level requirement and say it is not secure even though it may pass testing. Then it is not going to pass."

Dr. Schutzer offered his support for an innovative software-independent source for verification as opposed to legislation requiring a voter verified paper audit trail.

Ms. Quesenbery asked Dr. Rivest to comment on complexity as the enemy of security.

Dr. Rivest noted that as we add requirements, software becomes more complex. "The goal here would be software independence all around so that any voter can audit their vote in a way that would allow them to be as independent as possible from the software of the system."

Ms. Quesenbery asked if that separated the input mechanism from the counting mechanism. “If there is a verification step of some kind in the middle, does that suggest that the input mechanism could be more complex and not damage the security of the system?”

Dr. Rivest responded affirmatively. “If you have a verification step in the middle of the process, then I think you obviate the need to trust the software of the input process as much. So, you end up with software independence in a nice way.”

Mr. Miller had two questions related to software independence. “Is a voting system software-independent when it is used in the field (1) if the system is not audited, or (2) when the people voting on the system, probably primarily because of disabilities, aren’t able to verify that what was put on the ballot in the first place was in fact what they intended?”

Dr. Rivest answered yes to the first question. “The system is SI if it produces evidence that is capable of being examined afterwards. It is a capability of being audited that we are talking about here. The auditing procedures themselves are outside the scope of what this Committee does. We don’t specify audit procedures.” With respect to the second question, Dr. Rivest noted that the current definition for SI refers to the ability of nondisabled voters to verify their votes.
The intent is to make the system be SI for all voters, and we can modify the definition under discussion as appropriate.”

Mr. Miller followed up with his concerns with voting systems that are likely to be used by only disabled individuals. “The ballot marker devices come to mind. In that case, even though they in fact produce paper that theoretically could be verified, unless you are able to visually see the paper and handle the paper, you would not be able to verify it. Yet a person who is able to see the paper and handle the paper would not use that system. I’ll expand on that for a minute. I test and work with these systems. It takes a great deal of time to complete the process of voting by ballot using the ballot marker system. A nondisabled person who has the capability of voting much faster than a disabled person would not necessarily be using that device.”

Dr. Rivest shared Mr. Miller’s concern. “If you have a system which is designed primarily for voters with disabilities, I think this Committee then has the responsibility to try to figure out where the exact boundary of the envelope is. I think that the goal should be as much as possible for all voters that the voting system is software-independent. For some voters, you may need accommodation or other approaches to try to approximate that approach. I look forward to working with the Human Factors and Privacy subcommittee to figure out exactly how best to draw those lines.”

Dr. Wagner elaborated on Dr. Rivest’s previous comment. “I think the intent was absolutely that electronic ballot markers and electronic ballot printers would meet the SI requirements. I think of the SI requirement as a requirement that you be able to verify or to audit the overall election results as a whole. It is not talking about a specific right of any one particular voter. The SI requirement is talking about being able to verify the election results as a whole. For instance, if we are talking about voter verification as one approach to SI, it is likely that some voters will verify their vote carefully, and some may not verify it at all. That's okay. These systems can still provide software independence even if not all voters are doing that."

In further discussion, Dr. Rivest and Dr. Wagner agreed that the goal should be accessible software-independent verification for all voters.

Ms. Purcell noted that the SI recommendation to the EAC, if adopted, would pertain to future voting systems. "I would hope that we are looking forward to making significant changes for future election systems."

Hearing no further discussion, the Chair asked Mr. Eustis to read the resolution as proposed.

Resolution 02-06: Title: Software Independence in the next iteration of the VVSG
Offered by Dr. Rivest

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

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

After preliminary discussion related to interpretation of the resolution, the motion was seconded for further debate and amendment. In response to questions by various Committee members regarding current voting systems, Dr. Rivest clarified that an optical scan system and a DRE with VVPAT would both qualify as software-independent.

Several friendly amendments were offered by Ms. Purcell and Ms. Quesenbery and accepted by Dr. Rivest. Reference to "VVSG 2007" was changed to "next iteration of the VVSG," and "the TGDC directs NIST" was amended to read "the TGDC directs STS."

Referring to his experience as a tester of voting systems for ten years, Mr. Miller expressed his concern with the implications of the resolution on poll workers and election officials. "With the paper audit trail, we have added complexity for the poll workers to handle. We have reduced the reliability of the equipment in the field and from an election administration point of view; those are also important issues that need to be brought into play. I am concerned at this point that we are imposing a requirement before we have really proven that the pre-deployment testing and verifying processes that state election officials have used for a few decades is failing. Now we are adding another requirement that they also be able to not only test before deployment but in fact audit the system after they deploy it."

Dr. Rivest answered that adding an audit capability to the system adds additional work. "Testing provides some assurance that things may work well but it is not a panacea. You can't test every logic path through a piece of software. Testing is a tool but it does not provide the backup. When the audit trail is there, it provides a recovery capability. When you have something that has gone wrong, you have a paper trail or some other means of verifying the accuracy of the vote. If the testing fails to catch a bug, the audit trail provides a recovery mechanism that allows you to recover that vote in many, but not all, cases."

Mr. Berger expressed his discomfort with the focus of the current resolution as regards to superiority of one voting system over another. "It seems to me that the concept of software independence puts the focus one place where to totally improve the security of the system, we need to put all the voting systems under equal scrutiny. What we are really after is voting systems that are auditable and develop a permanent record. Obviously paper systems are arguably not a permanent record in that they can be compromised in a number of ways. You can swap ballot boxes, and you can destroy the paper in any number of ways. So as we craft this resolution, I would strongly recommend that we craft it in a way that puts equal pressure to have total system security equivalency as opposed to more dependence on physical security of the system."

Dr. Wagner stated his support for the current resolution. "I think the current Resolution recognizes the limits of the current state of the art in assessing the security of large software systems, and I think this focus on software independence is exactly the right one."

Hearing no further discussion, Dr. Jeffrey asked for a vote on Resolution 06-02 as amended:

Resolution 02-06 (As amended): Title: Software Independence in the next iteration of the VVSG Offered by Dr. Rivest

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

Therefore, the TGDC directs the (Security and Transparency Subcommittee) STS, in its development of the next iteration VVSG, to draft requirements for voting systems of the Software- Independent class, and not to draft requirements for voting systems of the Software-Dependent class.

A Committee member requested a roll call vote. Dr. Jeffrey noted for the record that eight votes are needed to adopt a resolution. The Chair asked Mr. Greene to call the roll. Resolution 06-02 failed to pass by a vote of 6 yeas, 6 nay and 2 abstentions (see Table 1).

The Chair asked Mr. Eustis to read the next motion into the record, inserting language corresponding to friendly amendments offered with the last resolution:

Resolution 03-06 (As amended) Title: The Innovation Class in VVSG 2007
Offered by Dr. Rivest

To spur development of new and innovative secure voting systems, the TGDC directs STS to include in the next iteration VVSG a new class of voting systems, referred to here as the "Innovation Class." The TGDC directs STS to investigate high-level guiding requirements for systems in this class for the purpose of providing system implementers with a path towards achieving certification to VVSG 2007. STS should also investigate approaches for reviewing, testing, and certifying systems in this class. These approaches could include convening a review board to review submissions and performing expanded open-ended vulnerability testing on systems submitted for certification.

Dr. Williams seconded the motion.

Hearing no questions or comments, the Chair entertained a motion to accept resolution 03-06 by unanimous consent.

Dr. Williams moved that the motion be adopted by unanimous consent. The motion was so moved (see Table 1).

The Chair asked Mr. Kelsey of NIST's Information Technology Laboratory to provide a status report on electronic independent verification of voting systems. Mr. Kelsey posed the question, Can we write standards for all electronic voting systems that are auditable? He then reviewed various voting systems and proposed auditing techniques. Mr. Kelsey concluded that auditable electronic voting systems are worth continued investigation. However, at this time, writing specific standards to ensure security of the voting system is not possible. (Mr. Kelsey's entire presentation is available for review at: http://vote.nist.gov/ElectronicIDV-status-presentation.pdf.)

Mr. Patrick Gannon asked Mr. Kelsey if he was aware of any auditable electronic voting systems that did not use paper.

Mr. Kelsey answered that the Scytl voting system in Spain employed a dual process model without paper.

Mr. Gannon indicated that the United Kingdom was undertaking a series of election pilots with paperless systems. Mr. Kelsey stated he would research these methods.

Mr. Kelsey then began a review of the proposed security architecture for the next iteration of the VVSG. He indicated the goals of the team to write a standard that leads to a secure voting system- one that blocks attacks. In addition, the requirement must be testable. In his presentation, Mr. Kelsey gave an overview of:

- Security requirements and attacker goals/resources
- Voting system architectures
- Threats to voting systems.

He offered the following conclusions on VVSG2007 security standards:

- They will be based heavily on threat analyses drawn from extensive literature review, historical data, internal and external analysis, and workshops.
- Equipment, Documentation, and Open-Ended Vulnerability Testing requirements will fit together to improve chances of getting secure voting systems.

Mr. Berger asked Mr. Kelsey a question concerning the voting system clocks used when parallel monitor testing of a voting system is employed. “The clock should not tell the system what day of the month it is. It should be relative to the start of an election so that in testing, the machine would see exactly the same thing it would on Election Day.”

Mr. Kelsey indicated that this was a reasonable approach. He stated that he was unaware how amenable current voting systems were to parallel test monitoring. He noted that you would need to investigate network connections between voting systems.

There being no further comments, the Chair thanked Mr. Kelsey and adjourned the meeting for a one-hour lunch break.

December 4, 2006: Afternoon Session # 1

The Chair called the meeting to order and asked Mr. Phil Greene to call the roll.

Mr. Greene called the roll and reported fourteen members in attendance. He notified the Chair that the meeting could proceed with a quorum present.

Dr. Jeffrey then called on Dr. Nelson Hastings of NIST’s Information Technology Laboratory to
present an update on the security requirements for the next iteration of the VVSG.

Dr. Hastings thanked the Chair. He briefed the Committee on the following topics:

- Status of security requirements
- Approach to wireless communications
- New and modified requirements
  - Voter verifiable paper records (VVPR)
  - Securing electronic records
  - Setup validation.

Dr. Hastings covered the development process for the VVSG security requirements including review by the STS subcommittee. The draft VVSG security sections include:

- Access Control Requirements
- Cryptography Requirements
- Setup Validation Requirements
- Software Distribution and Installation Requirements
- System Event Logging Requirements
- Physical Security Requirements
- System Integrity Management Requirements.

Dr. Hastings reviewed issues related to wireless communication within voting systems. He explained the STS subcommittee recommendation that the VVSG prohibit wireless Local Area Networks (LANs) and Radio Frequency (RF) devices on voting equipment used to capture cast ballot records. He noted that this proposal would not impact T-coil wireless headsets. However, transmission of unofficial election results would require communication devices separate from the voting equipment.

Dr. Schutzer asked how the requirements differed from the VVSG 2005. Dr. Hastings noted that Infrared (IR) wireless technologies were permitted for the installation of software but not LANs or RF. Transmission of unofficial election results using LANs or RF would require devices separate from the vote-capturing equipment. “What we are doing by having a separate device is, we are providing an air gap between the voting system and the device that’s used to actually transmit the unofficial results. It does not provide a wireless capability into the voting system directly. That’s why we have this separation of two devices.”

Mr. Berger asked why the prohibition was specific to the vote-capturing devices and not the vote-accumulating equipment.

Dr. Rivest clarified that the recommendation is that wireless would be disallowed in systems that have counting capabilities as well as counting functionality. He then asked the Chair for permission to introduce the pertinent resolution at this time which would provide a focus for further discussion.

Without objection, the Chair agreed.

Resolution 04-06(Amendment to Resolution 35-05) Title: Wireless Security
Offered by Dr. Rivest

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

The Chair opened the floor for discussion.

Dr. Williams expressed a concern related to tradeoffs implied in this resolution. “A county the size of Fulton County has to prepare three thousand memory cards and keep them separated by precinct. It is quite a logistical effort. Whereas, with certain wireless systems, you can sit at a console in a shielded warehouse and program those three thousand voting stations from that single wireless location. So, we are giving up something here. Is what we are giving up worth what we are gaining? Have there been any instances of wireless actually being exploited?”

Dr. Rivest answered in terms of the two types of wireless systems. “Use of wireless technology for the kind of purpose to which you refer, does not seem to be very widespread. So, if you are asking about current exploits, I would view this recommendation more as a preemptive measure rather than a reactive measure. I think the distinction here would be between RF and IR. IR would be permitted to load the software in the fashion you described because IR can be shielded. It is line of sight. It can be shielded. With RF, there is no practical way to shield the building, and so that’s the basis behind the recommendation.”

There being no further comment, Dr. Jeffrey asked for a second to the motion to adopt resolution 04-06. The motion was seconded.

The Chair asked for adoption of the resolution by unanimous consent. Hearing no objection, resolution 04-06 was adopted by unanimous consent. (See Table 1.)

Dr. Hastings then reviewed proposed new and modified requirements related to voter verifiable paper records (VVPR), secure electronic records, and setup validation. He enumerated pros and cons for various VVPR records and additional recommendations including:

- Paper Rolls
    - Pro: Difficult to add or remove cast ballots
    - Con: Potential violation of privacy and usability/accessibility issues
    - STS Recommendation: Allow paper rolls with improved security and usability

- Bar Codes
    - Pro: Makes scanning paper simpler
    - Con: Voter cannot verify contents
    - STS Recommendation: Allow bar codes
    - Audit procedures must not depend on bar codes.

- Additional VVPR Recommendations
    - Require better documentation and tools including auditing software
    - Look at entire voter process accessibility
    - Enhance reliability of printers, and
    - Associated mechanisms.

The Committee engaged in considerable discussion exploring these matters. At the request of Dr. Williams, Dr. Rivest clarified recommendations related to improved security and reliability. “So, the idea is basically to make the housings for the paper rolls clamp shut securely so that it is evident if there has been an opening of the paper roll housing. With respect to usability,
election officials should not have to get a big long table and scroll open the paper rolls. They ought to have some mechanical aids for dealing with the rolls. Usability may also extend to making sure that the software used to actually configure the information that gets printed on the paper rolls is easy to use and works reliably. For example, if you have a multi-precinct polling site, at a minimum, you want information printed on the paper records for each ballot basically indicating which election it was used for, so that you can at least audit with some precision at that point. In addition, the software and the documentation for printing out those reports have to be easy to use and well-understood. Election officials have to be able to use it readily and come up with the proper configuration. So usability extends to the information for the poll workers as well. Election officials and poll workers end up as system administrators. The equipment has to be reliable and it has to be usable. When you tear off the paper roll, it should not cause the paper to accordion.”

The discussion then turned to thermal paper and printer quality. Dr. Schutzer indicated his displeasure with paper rolls for future voting systems. He offered a resolution to ban paper rolls in the next iteration of the VVSG. Dr. Williams countered that it might be more profitable to have the STS subcommittee fully investigate the issues before mandating a prohibition.

Ms. Quesenbery offered her viewpoints. “It seems to me this is a place where the intersection of security and core requirements is really an issue. Certainly on HFP, our predilection has been to try to write performance requirements rather than actual design requirements. If, in fact, we think that cheap thermal printers do not have a high enough reliability, then this should be covered by reliability requirements, not by banning thermal printers. It might be something that the STS and CRT committees ought to work together on to make sure that the CRT requirements are sufficiently strong and are specifically addressed. We do this in HFP where we started with accessibility requirements in the VVPAT section and made sure that the two sections coordinated properly.”

The Committee then debated issues related to the use of bar codes along with human-readable text on VVPATs. Dr. Rivest framed the dilemma for states with a recounting with VVPAT paper rolls. “I do want to point out that in a routine one percent audit, you could not use the bar code. You would have to establish that the bar code does match the human-readable content. However, in the case of a recount, it seems as if providing the option of having a capability to scan in the bar code would be very valuable. Some states that would recount the paper might want to use that option.”

In answer to a concern by Mr. Miller, Dr. Wagner elaborated on the issue.” This is a complicated subject. Bar codes are tricky to use for the purpose of audits. There may be some cases where you could use them. I think it’s going to depend heavily on the purpose of the audit. If the reason why you wanted to do a four percent audit instead of a one percent audit is to get a higher degree of statistical confidence that the voter verified records matched the electronic records, then you need to audit it manually. On the other hand, if you are doing the audit for some other purpose, if the failure mode you are worried about is not a mismatch between the electronic and the paper records but some other kind of failure mode, then you may indeed be able to use the bar code.”

Lengthy discussion continued, and Dr. Schutzer was not persuaded that thermal paper printers served either the voter’s privacy or accuracy in recounting. He then offered the following resolution:

Resolution 05-06 Title: Prohibition on Continuous VVPAT Rolls
Offered by Dr. Schutzer

VVPATs using continuous paper rolls are prohibited in the next iteration of the VVSG.

The resolution was seconded for discussion.

Ms. Purcell asked the Committee to consider recommendations of alternatives.

Dr. Wagner indicated that this would be a flat sheet of paper with one sheet per vote record. Dr. Williams and Mr. Miller noted that only two vendors currently provide VVPAT systems with this type of VVPAT capability, but no current large-scale implementation.

After a discussion of the pros and cons of current paper roll systems is use, the sense of the Committee was to withdraw the resolution for redrafting to better incorporate usability and security concerns.

There being no further discussion, resolution 05-06 was withdrawn, and the Chair asked Dr. Hastings to continue with his presentation.

Dr. Hastings covered the goals for new requirements to secure electronic voting records:

- Secure electronic records from voting equipment to central tabulation equipment.
- Prevent alteration or backdating of electronic records.
- Provide signed cast ballots and totals from voting equipment to support canvassing.

He concluded with an overview of new software validation requirements including:

- Documentation requirements
- A model setup validation process
- Inspection of backup power supply
- Inspection of cabling connectivity
- Inspection of communications
- Inspection of consumables
- Inspection of calibration of components
- Inspection of external interfaces
- Checklist of other voting equipment properties to be inspected
- Record creation of the inspection results.

(Dr. Hastings entire presentation is available at: http://vote.nist.gov/SecurityRequirementUpdate-presentation.pdf .)

Dr. Williams expressed concerns over requirements to which the laboratories could not test. “A voting system test lab cannot test for consumables in the precinct.”

Dr. Hastings clarified the requirements intention for laboratories to test for the capability of a voting system to depict the level of a particular consumable such as ink.

Mr. Berger asked Dr. Hastings whether authentication technologies in use today have been considered. “I am aware in some devices now, even I-Pods, there is technology to prevent any software that has not been authenticated by the right authority from being loaded. Have you explored that concept here?”

Dr. Hastings indicated that the NIST staff is currently examining these capabilities.

Hearing no further comment, the Chair noted for the record that NIST believes the preceding preliminary reports of technical support titled: Security and Transparency Subcommittee (STS) preliminary reports for the next iteration of the VVSG 2007 respond to eleven TGDC resolutions. Unless there are supplemental directions or corrections, the technical support and related work product will continue to be developed consistent with these preliminary reports. The Chair entertained any further questions, directions, or corrections.

Dr. Rivest expressed his concern over the lack of direction for NIST staff as a result of the failure to adopt resolution 02-06. “Given the failure of the SI motion to pass, I don’t know where we are left with that issue. We need to have some more discussion about that. So I would seek guidance from the TGDC as to what we do in that area.”

The Chair indicated that the Committee should be prepared to discuss these mattes further at a later time. He then called on Dr. Alan Goldfine to introduce the Core Requirements and Testing Subcommittee preliminary reports.

Dr. Goldfine thanked Dr. Jeffrey. He provided an overview of the CRT topics including:

- Electrical/Electromagnetic Requirements
- Reliability (including Quality Assurance/Configuration Management)
    - International Organization for Standardization (ISO) 9000/9001
- Accuracy and Reliability Benchmarks, Metrics, and Test Methods
- Commercial off-the-Shelf (COTS) components
- Conformity Assessment, Scope of VVSG testing
- Coding Conventions and Logic Verification
- California Volume Reliability Testing Protocol.

With respect to reliability, Dr. Goldfine noted that Dr. Flater will discuss an approach that departs from the current 'Mean Time Between Failure (MTBF)' metric in the current VVSG. The new approach would integrate the testing for system reliability into the test method proposed for system accuracy. Dr. Goldfine offered for consideration the use of an accepted quality assurance standard in the next iteration of the VVSG. "We have discussed an approach that
would require voting system vendors to implement a quality assurance program that is conformant, within the appropriate scope of operation, to the ISO 9000/9001 standard."

(Dr. Goldfine's entire presentation is available for review at: http://vote.nist.gov/CoreRequirements-part1-presentation.pdf .)

The Chair opened the floor for Committee members' questions.

Mr. Berger stressed the importance of the quality assurance manual and its contents. "When you start writing quality assurance manuals, you are going to get deep into vendor processes, and it is going to be important that those processes be understood in detail so that they are harmonious."

Dr. Goldfine indicated that one approach would be to write requirements so that when the process manual is written, the requirements will support the necessary goals for effective testing and certification.

Mr. Berger agreed and also noted that ISO 9001 compliance would involve added costs for the vendors. "I think we need to see a cost-benefit analysis as to whether that specific third-party audit brings sufficient benefit for the cost."

Dr. Goldfine referred back to the TGDC discussion during the debate of Resolution 30-05. "It was pointed out at the time that NIST really wasn't the right organization to conduct such a cost-benefit analysis."

Mr. Skall agreed that compliance cost is an important and difficult question. “I think the only alternative we really have in writing a standard is to say something like implementation shall conform to ISO-9000. “I think the question of third-party versus self-declaration certification is one for the EAC to decide. It is not the type of requirement you would put in the standard itself. I think the question we have in front of us is, should we put in a requirement for conformance?
That alone has cost implications but we really will not know the cost implications until we know how the certification is done. That’s sort of outside our control.”

Mr. Gannon inquired as to the coordination between the CRT and STS subcommittees on a firm requirement for the use of an open-format election markup language (EML).

Mr. Wack elaborated on NIST’s efforts to date. “There would be great benefit if ultimately all voting systems could produce records in a common format and EML seems to be one of the best choices. So, yes, we are very definitely considering that and we are working closely with CRT on that.”

Dr. Jeffrey inquired as to the potential benefits of ISO certification. “Are there enough examples from other fields where you can show the benefit of employing an ISO in terms of end-to-end systems which might include things like security, reliability, and other issues separate from cost benefit? And what specific guidance do you need from the TGDC on this matter today.”
Dr. Goldfine noted the aviation and automotive industries as examples. “What we propose to do is take the crucial procedures from the ISO-9000 approach and specify them as a series of requirements within the next VVSG.”

Without objection from the TGDC, the Chair noted that the intent of the Committee was in fact to move away from a vendor-specified quality assurance format and towards an overarching format in the next VVSG.

The Chair thanked Dr. Goldfine and adjourned the plenary meeting for a fifteen-minute break.

<u>December 4, 2006: Afternoon Session # 2</u>

The Chair called the meeting to order and opened the floor to Dr. David Flater of NIST’s Information Technology Laboratory to present part two of the preliminary report of the Core Requirements and Testing Subcommittee covering reliability and accuracy issues.

Dr. Flater thanked Dr. Jeffrey and provided an overview of his presentation on reliability and accuracy benchmarks, metrics, and test methods which included:

- Background
- New reliability benchmark
- New reliability test protocol

- Accuracy.

As background, Dr. Flater offered several basic definitions. “First of all, the word “benchmark” has a carefully written definition stating a “quantitative point of reference to which the measured performance of the system or device may be compared.” In plain language that means when we say benchmark, we are talking about a number in the requirement such as 163 hours. The word “metric” refers to a measure that we use to describe the performance of a system. For example, when we are talking about reliability, the metric that has been used up to now has been “mean time between failure (MTBF)” which is time divided by the number of failures. When talking about accuracy, we talk about a metric ballot position error rate, which is the number of errors divided by the number of ballot positions. There is also a metric for ballot mis-feed rate which is specified in VVSG 2005; however, there is not a test method specified for that benchmark as of yet.”

He then gave an overview of the “big picture” issues:

- In most cases, conformity to strict benchmarks cannot practically be demonstrated through operational testing.
- Lax benchmarks do no one any good.
- In other industries, performance to strict benchmarks is achieved through the application of available methods for design, quality assurance, and performance monitoring.
  - Functional failure analysis
  - Operational testing is only a validation of the design.

Dr. Flater noted that VVSG 2005 permits test labs to bypass portions of the system that would be exercised during an actual election by using “a simulation device… provided that the simulation covers all voting data detection and control paths that are used in casting an actual ballot.”

He then reviewed the MTBF benchmark in the VVSG. “A lot has been said about the 163 hours and that this is, according to most reviewers, wholly inadequate. As it happens, the benchmark that is demonstrated in the testing is not that. The mean time between failure that is demonstrated by the testing that is specified in the standard ranges between 44 hours and 73 hours at 90% confidence. The minimum duration of the test using the protocol that is specified in the standard to demonstrate that is 169 hours. That was increased from 163 hours as of 2005 as a result of a new calculation of the numbers that were in there.”

Dr. Schutzer asked whether the benchmarks were drawn from actual testing or derived from the actual specification. Dr. Flater indicated that the numbers were drawn from the specification. Dr. Schutzer indicated that it would be interesting to know realistically if these high failure rates were actually experiences.

Dr. Wagner commented on the experiencing of reliability testing in California. “When California conducted its first volume test, they were able to get a pretty good measure of the reliability of the voting system in circumstances that probably would be representative of a real election. It was an actual test of the full system without this simulation bypassing the user interface. My rough estimate from the data that we got of the reliability of those machines which had been approved by the testing labs was about 15 hours MTBF. So that works out to a probability failure during one day of election operation of over 50%. This is only one data point and is not typical of most machines. In this one case, the kinds of failure we are talking about were paper jams and freezes of the machine, crashes essentially. Whether those could be recovered from depend on your procedures.”

Discussion followed among Committee members on types of failure and assumed statistical distributions (exponential). Dr. Flater agreed that the failure rate would be different for other distributions. Dr. Schutzer asked if availability would be a more useful metric than MTBF. Dr. Flater responded. “The advice that we received during the review cycle for VVSG 2005 essentially said this is not useful to include in the standard because this analysis assumes that you would be repairing equipment and putting it back into service on Election Day. If you actually do this, as an election is in progress, you have problems proving this was not an act of tampering. There are different ways to address the reliability problem. You can treat voting systems as consumables. They burn out in one day and then you replace them. If you want, you can do that. Being responsive to the feedback that we have received so far, what we’ve heard is that we would like higher reliability.”

Mr. Berger pointed out the importance of the fail-safe mode. Dr. Flater noted the general requirements that no votes shall be lost. Dr. Schutzer introduced the concept of the vote as a transaction. Dr. Flater noted an issue with fleeing voters. Dr. Williams elaborated. “A transaction on a voting machine occurs when you hit the cast ballot button. The way all of the current machines are designed, you would have to have an almost instantaneous failure at the time somebody pushed the button for that device not to record the vote. There are two schools of thought on the fleeing voter. One school of thought is that if you leave the voting machine in a suspended state, you just cancel the vote because otherwise someone would be voting for you. If you want to talk about fraud, I could certainly go through your ballot and change anything in there I wanted. The other school assumes that whatever is in that machine is the intent of the voter, and you should cast it. I know of states that have both of those laws. Some cast the ballot for the voter that fled. Some cancel the ballot. On the matter of the transaction, the way the current machines are designed, it would be an unusual circumstance where you actually lost a transaction.”

Dr. Flater then provided data on a more stringent benchmark for MTBF. “We have received some advice regarding what the mean time between failure benchmark should be. The lowest level was that MTBF should be 1500 hours which would give a 1% probability of failure during a 15-hour election day. Using the same test protocol and same parameters, if we want to give 90% confidence that the system conforms to that, we are looking at 234 days of test time which means, if you want to get it over with in a week, you need 34 devices running parallel. If you happen to have 100 devices as in the California reliability testing protocol for DREs, you have to rack up 2.34 days of run time. This is already 9 times as long as the California volume tests as specified." Dr. Flater noted that the 1500 hours originated in an IEEE P 1583 draft voting standard and was later increased to 15,000 hours. "We are in the realm where it is quite realistic to ask the question whether practically we can rack up this much run time with real voting systems."

Dr. Flater summarized methods for more realistic volume testing including eliminating lax benchmarks, eliminating tolerance of failures that occur during testing, and making full use of data collected throughout an entire testing campaign. However, we must acknowledge that quality cannot be tested in, it must be built in. Our ability to demonstrate reliability and accuracy during a test campaign of reasonable length is quite limited. So, if the goal is to have a reliable voting system, it's going to require changes in the entire process."

He then offered the outline of a new volume-based reliability benchmark:

- Time-dependent: continuously moving parts, perishable substances
- Volume-dependent: parts that move when something happens, certain software failures (e.g., crashes due to memory leaks)
- MTBF says nothing about the workload
- Equipment is unlikely to fail with no workload.

He noted that benchmarks can be specified for different types of devices according to whatever concept of volume or time is most appropriate. "We can specify volume in terms of the number of ballots or ballot positions or whatever, and also any assumptions that would also affect the way the system performs. Given these numbers, we can calculate a benchmark. If you only want one benchmark, then we need to choose the proportion of devices that fail as well as a measurement of volume to be applicable for all devices. Alternatively, you can specify one kind of benchmark for vote capture devices and another kind of benchmark for central account tabulators."

Dr. Jeffrey inquired whether performance data indicating failure rates was available from the last election. Commissioner Davidson indicated that while there was no data available at this time, collection would begin with the new EAC laboratory certification program in January 2007.

Dr. Flater then presented issues related to current and future reliability test protocols. "The bottom line currently is that up to 6 failures are tolerated during the testing campaign. Of course, you cannot expect the performance of the equipment after it is fielded to be better than what you saw during testing. A trickier problem is the assumption of the self-contained test. If you look at the current standard, it seems to say clearly that the testing for the evaluation of reliability and accuracy is done concurrent with and exclusively within the environmental testing for temperature and power variation tests. This was convenient at the time because the test runs for a certain amount of time that is commensurate with the test protocol for reliability. But this leaves us in a bind if, supposing the equipment does fine during that particular phase of testing, we start seeing failures in other parts of the test campaign. Presently, as far as I can tell, there is no protocol in the standard telling the test lab how to consider failure that occurs elsewhere in the test campaign."

He then offered for discussion some possible changes to the current reliability test protocol:

- Collect data across all valid system tests
  - To include at least one good volume test
  - Ignore tests where simulation is required (e.g., for safety of personnel) or when errors are forced
- Reject if data collected show with 90 % confidence that the system does not conform
  - Even on a single failure
- Report the performance that was demonstrated with 90 % confidence
  - Varying with length/volume of testing, number of failures observed, etc.
- Do not require exhaustive testing.

Ms. Quesenbery inquired as to testing of voting systems for disabled voters. "An accessible voting system is really multiple systems in one because it is not only the visual tactile interface, for example, but it might also be an audio tactile interface. Would that require two separate tests or is that a single test?"

Dr. Flater believed that these extra interfaces which attach to a DRE voting system presumably would all be considered components of a DRE. "Over the course of the test campaign, you would test these various different interfaces so the reliability observed of these components would have an impact on the reliability observed of the DRE."

Ms. Quesenbery also remarked on the need for diversity when constructing a volume test for voting equipment. "For the reliability test, it probably does not matter although if the point of having a real human is to generate diversity of human behavior in dealing with voting machines, then you would want to make sure that people of different ages, different language abilities, and different physical abilities were all included."

Dr. Flater concurred.

Mr. Berger commented that he believed the test lab should record any failures, no matter where they happen in the test campaign. "If the testers start to see a pattern, then that is cause for investigation into the underlying causes. I have seen where sometimes there is a latent defect that does not show up for some time. I think certainly if there is an observed pattern of failure anywhere in the test campaign, that it is certainly appropriate for the pattern to be explored and potentially cause a lab to fail a voting system."

Dr. Wagner then provided his feedback on reliability benchmarks. “You asked about the tradeoff between the benchmark and the testing methodology. I think we would be best serving our voters by focusing on proving the test methodology as our first priority and making only modest improvements on the benchmark number. We may also want to take into account the varying impact of failures on different voting classes. For instance, if a failure occurs and an op-scan machine is rendered unusable, voters can continue voting, and the ballots can still be accepted. The impact in this instance is not absolutely devastating. In the instance when a DRE fails, then the machine is unusable. Now all of a sudden voters cannot vote on that machine, and the impact may be more severe.”

Dr. Schutzer highlighted the need to consider the nature of the failure and whether the voting system is recoverable or not.

Dr. Flater then reviewed issues related to the accuracy benchmark. “The issues here are not with the benchmark so much as with the way the metric is defined. We still have the issue with the simulated volume and with the validity of the system test. We want to make the same changes here. The metric that is in the standard is ambiguous in terms of confusing ballot positions with the votes.”

Dr. Schutzer began a discussion on a more comprehensive test inclusive of both accuracy and availability benchmarks. Ms. Quesenbery expressed skepticism in designing an all-inclusive test.
“The whole point of the usability test towards which we are working is to be able to have a benchmark for minimum error rates, but I’m not sure that this same test will give you both the volume for reliability and accuracy and also human performance errors.”

Dr. Flater then began an overview of COTS issues. “The guidelines are confusing on the subject of COTS and, in places, possibly even self-conflicting, but COTS are not exempt from test lab scrutiny. A part of this confusion, I believe, results from terminology, trying to characterize everything as either COTS or not COTS.” He then offered a relevant definition for COTS as it relates to voting systems:

- COTS: Software, firmware, device, or component that is used in the United States by many different people or organizations for many different applications and that is incorporated into the voting system with no vendor- or application-specific modification.

Dr. Flater then elaborated on the implications of the definition. “COTS are not automatically excluded from anything except the requirement to deliver source code and that’s for pragmatic reasons. Having received a voting system to be tested, the test lab must make a determination whether previous certifications and field experience render any portion of the test campaign redundant. If, in fact, there is a piece of COTS that arguably has already been demonstrated to satisfy the requirements of the guidelines and is suitable for use in voting systems, that would feed into this determination. However, any reduction in the scope of testing must be justified in a test plan and approved by the

EAC. So this is a controlled process. Nothing is going to be automatically excluded from scrutiny."

Both Dr. Rivest and Dr. Schutzer inquired into the specifications for "black box" testing of a COTS product. Dr. Flater indicated that the product would be tested as part of the entire voting system. "If there is a need for more focused testing of just that part of the system, that is something we need to discuss further."

Dr. Wagner offered his concerns with regards to the introduction of malicious code or 'Trojan horses' into COTS products. "One thing to note from the security field is that you, generally speaking, cannot detect Trojan horses using black box testing alone. So the concern would be that testing labs might be unable to tell whether or not malicious code was present when they would only be doing black box testing because they don't have access to the source code. If the outcome of your election is dependent on the correctness of the software, then malicious logic in COTS code might be a problem because it might go undetected."

Considerable discussion ensued on the matter of testing COTS and the security issues inherent in the use of this software in voting systems. No consensus was reached. Dr. Rivest offered some perspective. "Maybe I could comment about exactly what 'commercial off-the-shelf' means these days. I mean if you are talking about something that you pay for, that is one thing. If you are talking about software you download from the web, that is a big shelf out there and there is lots of stuff on it."

Mr. Berger elaborated on previous relevant CRT subcommittee discussions. "We also had some conversation there about having some assurance that the generic use of the COTS was sufficiently close to the use in the voting system that there would be some confidence that, in fact, it was fit for use."

Dr. Flater offered additional output from previous CRT discussions. "Another idea that came up in the discussion of COTS was the opportunity for the EAC to maintain a list of COTS products that were previously found to have been acceptable for use in voting systems. This list would be input into the determination of a test plan, specifically the work that the test lab would have to do to ensure that the use of the COTS product in a new system is comparable to its use in the previously approved system. If it is not comparable, then nothing from the previous approval would be applicable. In any case, there would be no waiver from system testing. You always test the entire system."

Dr. Flater then moved on to a brief review of coding conventions and logic verification. He prefaced his presentation remarking that the directions taken on coding conventions and logic verification issues are unchanged since they received general approval at the September 2005 TGDC meeting. He then outlined the directions taken:

- Expand coding conventions addressing software integrity (the 20 % with 80 % impact)
  - Start with IEEE P 1583 requirements

  - Make defensive coding requirements more explicit
  - Require block-structured exception handling
- Clarify length limits (modules vs. callable units)
- Require use of “published, credible” coding conventions instead.

He also offered a similar opportunity for EAC involvement where the Commission could periodically review current best practices and publish a list of coding conventions acceptable for use in voting systems.

Dr. Wagner and Dr. Flater discussed at some length the prohibition of C as an acceptable programming language. Dr. Wagner offered his perspective. “There are good reasons why operating systems and imbedded systems are often written in C language instead of, for instance, C++ or other higher-level languages. I wonder whether it’s really necessary to forbid C to get the good things you want. There are extensions to C -software packages- that can provide structured exception handling. So, I wonder whether it is really true that this new requirement actually does rule out C. If it does rule out C, I think the cost of that may be very significant.”

Dr. Flater agreed that the use of the extensions could well be a credible path to follow. He agreed to research the extensions and modify the restriction on C as appropriate.

Dr. Flater concluded the afternoon presentation with an overview of logic verification issues. “Logic verification tries to do an analysis of the source code to generate confidence that it will be correct in all cases. The motivation for this verification was a TGDC resolution asking for a higher level of assurance in operational testing alone and, as well, to clarify the objectives of the source code review.”

He discussed potential compromises that would allow for realistic verification. They included limiting the scope of verification to core logic that is responsible for vote recording and
tabulation. He noted that this approach could be attacked as either too rigorous or not rigorous enough.

Dr. Jeffrey thanked Dr. Flater for his presentation. (The entire presentation is available for review at: http://vote.nist.gov/CoreRequirements-part2-presentation.pdf.) He then asked Committee members to think carefully about issues discussed today. “In the first slide that was shown this morning where Commissioner Davidson showed the schedule for the delivery of the next iteration of the VVSG, you will notice that on July 31, 2007, the TGDC should forward the draft VVSG to the EAC. If we end tomorrow with a lot of open issues, we are not going to get there. So, I urge you, as you are having dinner tonight, to think about additional open issues and see how many of those that we can close tomorrow to provide the guidance necessary to produce a really good draft by July.”

The Chair adjourned the meeting until 8:30 a.m. the next day, Wednesday, December 5th, 2006.

<u>December 5, 2006: Morning Session # 1</u>

Dr. William Jeffrey welcomed the Committee members and public for the second day of the seventh plenary session of the TGDC. After the Pledge of Allegiance, he called on Mr. Phil Greene to call the roll. Fourteen members responded present. (See Table 1.) Mr. Greene informed the Chair that a quorum was present.

Before proceeding with the presentation of preliminary reports, Dr. Jeffrey opened the floor for the introduction of resolutions.

Dr. Rivest brought forward a revised 'software independence' resolution. "I think we were close yesterday to passing a motion that would be supportive of the STS subcommittee's recommendation. We have a revised motion that we would like to submit. I think Mr. Paul Miller drafted the final wording of this resolution, and I think it reflects the concerns of those of you who voted no to the earlier motion. If not, I hope that a small modification of this would be sufficient to achieve your support on this issue. I feel this is an important motion for this Committee, and I hope that the revised version addresses the concerns of those of you who had concerns with the original wording."

Dr. Rivest introduced the resolution.

Resolution 06-06 Title: Software Independence of Voting Systems
Offered by Dr. Rivest

Election officials and vendors have appropriately responded to the growing complexity of voting systems by adding more stringent access controls, encryption, testing, and physical security to election procedures and systems. The TGDC has considered current threats to voting systems and, at this time, finds that security concerns do not warrant replacing deployed voting systems where EAC Best Practices are used.

To provide auditability and proactively address the increasing difficulty of protecting against all prospective threats, the TGDC directs STS to write requirements for the next version of the VVSG, requiring the next generation of voting systems to be software-independent. The TGDC directs STS and HFP to draft usability and accessibility requirements to ensure that all voters can verify the independent voting record.

The TGDC further directs STS and Core Requirements and Testing (CRT) Subcommittees to draft requirements to ensure that systems that produce independently verifiable voting records are reliable and provide adequate support for audits.

The Chair opened the floor for discussion.

Mr. Berger asked for more detail on the concept of software independence. "Would an implementation of the resolution that is model-driven, where specific coding is verified against a structured model, qualify as software-independent in your understanding?"

Dr. Rivest referred back to the definition of software independence. "If an undetected error in the software could cause an undetectable change in the election outcome: if you can match those words against your use of model-driven development, I think you should have an answer.
I think the answer is probably no unless there is some sort of auditability, because merely being model-driven, I think, does not provide the auditability that we seek in the resolution."

Mr. Berger offered the Committee perspective on the utility of 'model-driven architecture' relative to the specific software code that records and verifies a vote. "The software on a DRE or electronic voting machine that focuses on the critical element of what happens in the voting booth is less than a megabyte. That is not a lot of software. I have to believe we can verify and put very careful controls on that code so that we can get an accurate and verified record of what the voter does in the voting booth in multiple ways. The Object Management Group [a computer industry consortium, see: http://www.omg.org/] has done work in a number of arenas to get trusted and verified software. They have developed a robust model-driven architecture system with automated tools to verify software against the structured model to implement various processes. That to me offers a very promising way forward that is readily available. I personally think we owe it to ourselves and to those who use these voting systems to see if those tools may not solve the problems we are worrying about."

Dr. Schutzer shared his concerns with this approach given the state of the technology. He indicated that Internet browser software, while smaller than the vote-casting software, cannot be secured. "As a member of the financial services community, I can say we are all looking forward to the Trusted Computing Initiative, but to be honest, it is not here yet. No one is saying that the current DREs are not secure or cannot be made secure. What we are saying is that in today's state of the technology, we are unable to prove to someone who would challenge the DRE, that there was not something lurking there that was throwing the election, so to speak. I think over a period of time with innovation and advances in software, we may eventually get to the point where (a) the software could be proved secure, and/or (b) there might be secure electronic equipment. However, today in the here and now, if you really want to move forward, software independence would be the simplest, most pragmatic way to get it done."

Considerable discussion ensued on the issue of software independence as a safeguard. Mr. Berger noted the unique safety record and complexity of software in the airline industry. Dr. Rivest offered his view. "The airline industry has a wonderful record of developing software. They spend orders of magnitude more on their software than, I think, the voting industry is currently doing and would prospectively do. Moreover, I think you also have the problem of errors. If you have an error and a plane goes down, you know it. If you have an error in an election and the wrong person is announced the winner, you may not know it, and that's a very significant qualitative difference."

Mr. Berger provided the Committee with an overview of the Object Management Group's Model-Driven Architecture in the area of software assurance as it related to the current issue. "We need to focus the problem on specifically getting the voter's vote verified and unaltered out of the voting booth. That, I think, is a constrained problem that is much more tractable." (Mr. Berger's complete presentation is available at: http://vote.nist.gov/Berger1204OMGpresent.pdf .)

Dr. Schutzer expressed his concerns. "We have not yet reached a stage where, from a specification, we can automatically generate software code untouched by human hands and, therefore, free of error. I would say that life isn't perfect and, of course, the added complication, as I pointed out, is that we can build a lot of error control checking in our financial processes and in our airline industry because we do not have the problem of having to maintain the voter's privacy. We can carry through the details of a financial transaction or identification of all of the parties involved."

Both Dr. Schutzer and Mr. Berger agreed that a two-to-three-year time line for implementation of new voting systems was problematic and could stretch out to 2011. Dr. Schutzer also had concerns with the size and nature of the market for voting systems. "What we have is a federation of independent entities buying machines under some general guidelines. I would say it would be extremely hard to make that an attractive-enough marketplace."

Mr. Berger agreed. "Exactly because of these constraints, I think if we move to a model-driven architecture at critical points in the system, such as making sure we get a voter's vote recorded and verified and then unalterably delivered from there to the rest of the system, I think we can see economies of scale. I can also see verification tools developed to verify to that model."

Ms. Quesenbery asked if there was conflict between adopting software independence and model-driven architecture. Dr. Schutzer replied that he saw no conflict. Mr. Berger responded that model-driven architecture does not imply software independence.

The Chair called on Dr. Wagner to address the issue from a security perspective. "The STS subcommittee considered many of these issues at great length and came to a compromise which recognized the need for innovation. In fact, the full TGDC passed by unanimous consent a resolution yesterday to create an innovation class which would permit exactly these kinds of innovative approaches to be proposed and considered in the standard. I do not see any conflict here between the kind of approach that Steve Berger is talking about and the SI resolution in front of us."

Ms. Mason commented on the language in the current SI resolution on the floor for discussion. "After much consideration and talking to members offline, I think it is important that we reconsider this issue. I am really in favor of the fact that the human factors subcommittee's concern has been included to ensure that this sort of voting system will be accessible to all users. So, for the record, I am now considering a change of heart."

There being no further discussion, the Chair asked if there was a second to Dr. Rivest's motion.

Ms. Quesenbery seconded the motion.

Dr. Jeffrey asked if there was further discussion. Hearing none, he asked if there was objection to adoption of Resolution 06-06 by unanimous consent. With no objection, the resolution was adopted by unanimous consent. (See Table 1.)

The Chair asked Dr. Flater to complete his presentation of the preliminary report of the CRT subcommittee.

Dr. Flater provided an overview of conformity assessment and scope of testing issues. "The National Voluntary Laboratory Accreditation Program (NVLAP) accredits testing laboratories to perform conformity assessment. This means that the labs are assessing the adherence of the voting system product to requirements in the guidelines. It also means anything not specified in the guidelines is irrelevant unless it is required to test things that are specified. This process strives for maximum objectivity, repeatability, and reproducibility. It is an assessment measurement process."

Dr. Flater outlined the significant outstanding issues, including:

- The VVSG 2005 testing volume requires testing of vendor-specific functionality.
  – This is not conformity assessment
  – Not traceable to requirements of Volume

- Impossible to include all state-specific requirements in a federal standard.

Dr. Flater concluded with two points for further discussion:

- The Testing Standard of the Voluntary Voting System Guidelines shall not require the test lab to perform activities beyond the scope of assessing conformity to the Guidelines.

- This does not preclude the EAC from adding requirements and/or criteria beyond the VVSG for certification, nor does it preclude test labs from performing additional tests.

The Chair thanked Dr. Flater and called on Dr. Sharon Laskowski to present the preliminary report of the Human Factors and Privacy (HFP) subcommittee. (Note: Dr. Flater's complete presentation is available at: http://vote.nist.gov/CoreRequirements-part2-presentation.pdf.)

Dr. Laskowski thanked the Chair and provided an overview of the subcommittee's presentation:

- Changes in the VVSG HFP section
  - o Summary of the changes from VVSG 05 to VVSG 07. Most are clarifications and corrections.
- Research Progress
  - o A Report on two research projects to support further edits to the VVSG
- Issues requiring further analysis

  - Plans to examine a number of topics to support additions to VVSG.

Dr. Laskowski reviewed Chapter 3 of the draft VVSG document covering the human factors guidelines. She offered clarifications between the HAVA language and the VVSG requirements pertinent to scope and primary audience for each document.

Mr. Gannon commented on terminology here. “Under the characteristics of document scope, you list the VVSG as covering voting equipment. That term oftentimes implies hardware when, in fact, the VVSG, I think, is much broader than that. From my perspective, we need to refer to entire voting systems.

Dr. Laskowski and Ms. Quesenbery agreed to review the terminology to harmonize it with the VVSG document’s glossary. Dr. Laskowski then went on to show the proposed placeholders for performance benchmarks.

Ms. Quesenbery commented on the future benchmarks. “We have worked to try to make as many of the benchmarks performance-based as possible because we think that leaves it open to cross platforms of different kinds of input devices. However, there are places where we know some very specific things from prior human factors research. There we have included the design guidelines that were in the VVSG 2005, and they are noted by system class- whether it applies to a touchscreen or to paper or to whatever kind of input device is applicable.”

The Committee discussed at some length requirement 3.2.2.2 relating to notification of overvoting, specifically the language dropped from the VVSG 2005 allowing for disabling this function on optical scan systems with non-editable interfaces. Ms. Quesenbery elaborated. “I would also note that what we are talking about here applies to paper op-scan ballots because an electronic interface has the ability to manage this in a much different way than a paper ballot does. So we split the two systems because the feedback and notification to the voter is so different. A computerized interface can actually prevent an overvote and can give you an instant notification of an undervote, which you can change immediately without having to re-mark your whole ballot.”

Dr. Laskowski reviewed the new requirement for systems to detect marginal marks. Mr. Miller asked about the methodology for determining a marginal mark. Dr. Flater noted that NIST staff discussed this issue with the vendor community. He commented that different voting equipment detects these marks in different ways. “We know that the boundary of where you go from marginal to non-marginal is going to depend on calibration. If the mark is marginal, we will give it back to the voter for clarification. The important thing is that we have eliminated the possibility of the voter accidentally getting a ballot into the ballot box where their intent is ambiguous.”

Dr. Laskowski reviewed new plain language requirements. “The plain language requirements were based on best practice in general, not on voting specific guidelines or experiments.” In response to concerns by Committee members over the use of election jargon, Dr. Laskowski referred to the requirement for ‘simple vocabulary’ that promotes the use of common words and the avoidance of technical terms.

Dr. Laskowski reviewed the adjustable font and contrast requirements. Dr. Williams noted that the HFP subcommittee should consider making these “shall” requirements, and adjustable during the length of the voting process. “You don’t want it to be an all-or-nothing decision by the voter right at the front end.”

At the request of the Chair and other Committee members, Ms. Quesenbery commented for the record that the Committee at this meeting was making recommendations for wording changes in the draft HFP requirements. As a result of these recommendations and further discussion within the HFP subcommittee, a final draft will be brought back for a vote at a future plenary session.
“What we want is a sense of this Committee on whether there are objections that we have not considered.”

Dr. Laskowski asked the Committee if a newly added requirement dealing with perceptual issues needed clarification:

3.2.4 - H. Visual Access to VVPAT

When the voting system asks a voter to compare two distinct records of his/her vote (as in VVPAT systems), both records shall be positioned so as to be easily viewable and legible from the same posture.

Dr. Williams agreed with the resolution and offered an additional consideration. “When you are comparing two records of your vote, shouldn’t these representations be in the same font sizes and the same contrast and the same language? If the intent here is for me to verify my vote, so to speak, I can’t very well verify it if I can’t read it.”

Ms. Quesenbery agreed and noted that the newly adopted software independence resolution provides a new mechanism for consideration of just these sorts of visual verification issues.

The Committee engaged in discussion of issues related to a voter keeping the same posture while verifying the vote. Also, Mr. Miller noted that the ballot on the DRE screen appears in a different format from the ballot choices on the VVPAT paper rolls. Mr. Wack offered his understanding of the STS subcommittee intent on this broader issue that would apply to all voter verifiable paper record systems. “If you are going to go through the trouble of having a VVPAT system, you have to come up with some way of facilitating the voter to actually do the comparison.”

Dr. Laskowski summarized new timing issue requirements dealing with how long the voting system and voter wait for each other to interact. The requirements included:

3.2.5.1 - A. Maximum Initial Response Time

The initial response time of the voting system shall be no greater than 0.5 seconds.

3.2.5.1 - B. Maximum Completed Response Time for Vote Confirmation
When the voter performs an action to record a single vote, the completed response time of the voting system shall be no greater than one second in the case of a visual response, and no greater than five seconds in the case of an audio response.

3.2.5.1 - C. Maximum Completed Response Time for All Operations
The completed visual response time of the voting system shall be no greater than 10 seconds.

3.2.5.1 - D. System Activity Indicator
If the system has not completed its visual response within 1second, it shall present to the voter, within 0.5 seconds of the voter's action, some indication that it is preparing its response.

3.2.5.1 - E. Voter Inactivity Time
The voting system shall detect and warn about lengthy voter inactivity during a voting session. Each system shall have a defined and documented inactivity time, and that time shall be between 2 and 5 minutes.

3.2.5.1 - F. Alert Time
Upon expiration of the inactivity time, the voting system shall issue an alert and provide a means by which the voter may receive additional time. The alert time shall be between 20 and 45 seconds.

Dr. Williams offered a recommendation relative to the range of times in the requirements. “On these recommendations where you give a range of time, does that imply that the system has the ability to set the time between those limits, or are you going to pick a time between those limits and put that in the standard? My recommendation, since I brought this up, is that you simply pick a time like 5 minutes- because otherwise you are building complexity into the system when you don’t really need complexity.”

Dr. Wagner saw value in the ranges to avoid an additional burden on the election official. “I think that it might be fine to have a range in the standard that allows the vendor to pick one rather than the standard saying it must be exactly 3 minutes because either way, neither would introduce a burden on election officials.”

Ms. Quesenbery and Dr. Laskowski agreed to take the preceding input from the Committee back for further refinement of the standard before the next plenary session. They agreed with Dr. Williams that the requirements should consider the poll workers that interact with the voting system as well as the voter.

Dr. Laskowski covered a clarification to the alternative language requirement. Dr. Williams remarked that the vendor declares what languages their system is going to support, and the system is then tested for only those languages.

The Committee discussed, at some length, the requirement for plain language as it might apply to alternative languages.

Dr. Laskowski reviewed new requirements dealing with usability of voting systems for poll workers and usability requirements related to system maintenance including documentation.
She indicated that these system maintenance requirements applied only to poll workers. Dr. Williams noted that this restriction on the requirements was important. “You specifically don’t want to include outside or vendor maintenance in this because any time a machine goes outside of your control, when it comes back, you have got to put it back through acceptance testing.”

The Committee engaged in discussion over voting system safety requirements and compliance with current regulations. Mr. Berger offered words of caution here. “We have very well-established safety standards typically certified by Underwriter Laboratories or similar agencies. I would really worry if we try and duplicate that effort in that we may get it wrong. We’ve got good existing standards; I think we ought to just cite them- such as the internationally accepted IEC product safety standard.”

Dr. Laskowski concluded the requirements portion of her presentation with a summary of updates to usability requirements dealing with (1) contrast and color for voters with partial vision, and (2) a space requirement for voting systems allowing for an assistant to assist a disabled voter. Dr. Williams suggested using the terminology “adequate access.”

The Chair noted that it was 10:15 a.m. and adjourned the meeting for a fifteen-minute break.

December 5, 2006: Morning Session # 2

The Chair recognized Dr. Laskowski. She summarized the human factors research progress to date. Highlights included:

- Usability benchmarks
    - Our preliminary results appear to confirm our hypothesis that we can define benchmarks.
    - Usability testing with our protocol and feasible sets of test voters can detect and measure error rates and discriminate among different implementations.
    - The protocol successfully measured time to vote and satisfaction; on these two dimensions, there were no significant differences between the two systems tested.

- Next steps
    - Additional experiments to determine benchmarks and test voter population to validate the test protocol.
    - Voting-specific plain language research has begun.
    - Experiments have been defined.

Dr. Laskowski then covered usability issues for the next VVSG that require further analysis and research including color and audio interface guidance. She noted that vote by phone and audio voter-editable ballot devices could benefit from research findings for Interactive Voice Response (IVR).

Mr. Berger inquired as to whether there was an option to allow high-contrast black and white displays to deal with color blindness issues. Ms. Quesenbery responded that this was in fact written in the requirement. Remarking on the importance of color capability within a voting display, she struck a cautionary note. “Not every voter thinks of making an adjustment, and they may not realize that they are seeing the screen inaccurately. So, you want to make sure that you have worked to make the screen display provide good contrast; for example, to ensure that you are not displaying light gray on dark gray, or that you are not displaying red on black. These are things that we know are bad. However, it is a little hard to quantify those into a testable requirement.”

Dr. Laskowski reviewed requirements related to the usability of technical documentation provided by the vendor followed by design requirements for accessible voting devices. “Having design guidance in an accessibility standard for the accessible voting station is not necessarily sufficient to ensure good usability of those accessible voting stations. It does not necessarily guarantee that the people using these alternative accessible methods can vote in a timely fashion with few errors. We think it is really important to look at how to do usability testing for the accessible voting station. In addition to that, the benchmarks are going to be different for audio versus video. With audio, voting is going to take longer because you have to listen. Visual is quicker.”

Dr. Laskowski concluded her presentation with an overview of issues that will require collaboration between the three working subcommittees including:

- As security requirements are further developed, it is critical to consider impact on usability and accessibility,
    - E.g., issues for software independence, paper-based approaches.

- Holistic approach: We plan close collaboration between STS, CRT, and HFP.
    - Helps to identify and articulate key issues.
    - End-to-end accessibility for the voter process: can we develop a requirement to show that the entire system is accessible (the highest standard) or show how reasonable accommodation can fill gaps for full accessibility?

Dr. Schutzer agreed that collaboration would be critical to moving forward in development of the next VVSG. He offered another issue that would benefit from review by the subcommittees in concert. “We want to really examine the lessons learned from this last election and really look hard at the requirements that we are generating now, in terms of seeing what we could do to solve any problems that cropped up at the last election.”

Ms. Quesenbery agreed and offered another worthy item for further research. “We have been talking about doing some research into the use of icons, just as we have been looking at what plain language makes voting instructions clearer. Expanding on this idea, where, when, and how do icons and images actually help improve the clarity of the voting process for voters? I would like to get those exploration questions onto the list, certainly starting with some desk research if not moving into something with performance research.”

Mr. Pearce offered his concern with the use of the word “average” in the poll worker usability requirements. “There is one term about ease of normal operation that reads, ‘easy for the average poll worker.’ Is that a reasonable description? If I am by myself as the poll worker and I am trying to do this task, and it says it should be easy for the average poll worker. If I can’t do it, does that make me an idiot? That’s a concern.”

Dr. Laskowski and Ms. Quesenbery agreed to consider the use of the word ‘typical’ to replace ‘average.’

Dr. Jeffrey thanked Dr. Laskowski for the reports of the HFP subcommittee. (Dr. Laskowski’s entire presentation is available at: http://vote.nist.gov/HFP-progress-presentation.pdf.) For the record, he stated, “The Human Factors and Privacy Subcommittee believes that the proceeding preliminary report that they have just provided corresponds to nine different TGDC resolutions. Unless there are supplemental directions or corrections, taking into consideration the discussions that we have been having at this meeting and been taking good notes on, the subcommittee will continue to develop the products consistent with the preliminary report and the discussions that we have had this morning.”

The Chair asked if there were further corrections or directions. Hearing none, he entertained a motion to accept the HFP preliminary reports. A motion was made and seconded. Dr. Jeffrey then asked the Committee if there was objection to adopting the motion by unanimous consent. Hearing no objection, the HFP preliminary report was adopted by unanimous consent. (See Table 1.)

Dr. Jeffrey called on Mr. Mark Skall to clarify direction from the TGDC on an issue raised by Dr. Flater in the CRT’s preliminary report.

Mr. Skall thanked the Chair. He told the Committee that he wanted to make sure that we at NIST understand the direction that was given to us at this meeting, so we can perform the research and the drafting exercises correctly with respect to conformity assessment. “David Flater discussed a key issue about whether the testing standard should require the test lab to perform activities that are beyond the scope of assessing a voting system’s conformity to the requirements. At NIST, we have worked on many standards committees, and clearly testing laboratories, at least in our experience, always test to ensure that the requirements are met; nothing more, nothing less. David stated that the Testing Standard of the VVSG shall not require the test lab to perform activities beyond the scope of assessing conformity to the guidelines. However, there was no discussion. I want to make sure that he goes away with direction to proceed with that understanding if that, in fact, is what the Committee wants."

Dr. Schutzer indicated his concurrence. "I think the issue was in terms of what goes into the requirements that they test against as opposed to testing outside the requirements."

Ms. Quesenbery raised a related issue. "I know one of the questions that came up a couple of meetings ago was whether a vendor might want to ask the test lab while they are doing the conformance testing, to do other testing. Nothing precludes that, I assume?"

Mr. Skall answered affirmatively. "This does not preclude the EAC from adding requirements or criteria beyond the VVSG for certification. Nor does it preclude test labs from performing additional tests."

Mr. Berger offered a resolution for consideration by the Committee.

Resolution 07-06 Title: Guidelines & Federal Certification
Offered by Mr. Stephen Berger

To maximize the value of federal certification, the TGDC directs that observations collected throughout the testing campaign can be used to assess any requirement.

Further, the guidelines shall require that systems be tested to verify that all functions operate per the vendor's documentation and are reasonably fit for use.

Mr. Berger explained the intent of the resolution. "In my experience, it is very important to allow the test personnel to bring in failures that happen outside of the specific test regimen for a number of reasons, one of which is that sometimes stresses create latent failures that don't show up until later. It takes some further investigation to figure out why those things happen. The other point is that operational conditions will occur at random times, and until you construct the right test case, you won't reveal them. So, I think it is important to authorize testing outside the criteria for data that arise at any time during the test campaign."

Dr. Jeffrey inquired as to whether the proposed resolution implies that any additional functions that are included above and beyond the requirements have to be tested. Mr. Berger answered affirmatively that the functions would be tested for consistency and fitness for use.

Considerable discussion ensued on the two points within the proposed resolution. Mr. Skall expressed concern that anything related to certification is outside the scope of a standards document. Secondly, he remarked that ‘fit for use’ was a term of art. “How does one determine what fit for use is in a standards arena, where in fact we are testing for precise and exact requirements.”

Mr. Berger offered the example of the ISO 9000 standard where test labs evaluate the quality manuals from the manufacturers to determine if they follow their own documentation.

Dr. Williams noted that previous versions of the voting standards have contained the requirement that the system has to conform to its own documentation. “I think it should be included in the next standard because when the voting system comes out of certification testing, and I read the documentation, I want the conformance statement to imply that the voting system conforms to that documentation.”

Dr. Flater offered his concerns. “A general requirement saying that the system shall agree with its documentation is all fine and good. The issue is how we are going to scope the conformity assessment for that requirement. Once you go beyond the functions that are specified in the product standard, you are talking about open-ended testing. We must test every single function of the system, including vendor-specific functions for which there are no standards.”

Mr. Skall elaborated. “Let me try to summarize. One of the statements I made is that ‘fit for use’ is not a specific term. At NIST, we spend a lot of time writing precise, testable requirements. In the voting system’s documentation, a vendor may or may not spend a lot of time being precise. We want to verify that the system’s functions operate correctly. However, there are many ways to interpret a vendor’s documentation. So we get back into that same vagueness, in my opinion.”

The Chair recognized Commissioner Davidson. She remarked that the Committee needs to be aware of costs to the states for added testing requirements. The EAC does not want any of the states to drop out of our certification program. These added testing requirements are all good things. But they are going to push up the cost of testing a great deal. If we make testing of voting systems too expensive, the states cannot afford it. I don’t want any state dropping out of our certification program for that reason.”

After further discussion, Mr. Berger accepted friendly amendments. The resolution as amended read:

Resolution 07-06 (as amended) Title: Guidelines & Federal Certification
Offered by Mr. Stephen Berger

To maximize the value of federal certification, the TGDC directs that the guidelines be written so that observations collected throughout the testing campaign can be used to assess any requirement.

Further, the guidelines shall require that systems be tested to verify that all functions operate per the vendor's documentation.

Dr. Williams called the question. The Chair asked for a second to the motion to adopt the resolution. Ms. Quesenbery seconded the motion. The Chair asked if there was objection to unanimous consent. There was objection from a Committee member. Dr. Jeffrey asked Mr. Greene to call the roll.

Mr. Greene informed the Chair that the motion to adopt failed "six votes no, five votes yes, and one vote abstaining." (See Table 1.)

The Chair adjourned the meeting for a one-hour lunch break.

<u>December 5, 2006: Afternoon Session</u>

The Chair called the meeting back to order. He noted that this final session would provide Committee members with an opportunity to introduce new resolutions. He asked Mr. Greene to call the roll.

Mr. Green informed the Chair that with eleven members answering 'here,' a quorum was present. (See Table 1.)

Mr. Berger noted that in the interest of time and workload, he would withdraw from consideration the three draft resolutions circulated earlier to the Committee. These are the resolutions to which he alluded at the beginning of this plenary. Mr. Berger then indicated he would like to raise two additional resolutions for consideration. He deferred to Ms. Quesenbery while he compiled these resolutions for the laptop projector.

Ms. Quesenbery then offered a resolution for consideration.

Resolution 08-06 Title: Recommendation to ICDR
Offered by Whitney Quesenbery

The Interagency Committee on Disability Research (ICDR) sets the agenda for federal disability research and actively seeks recommendations for future research topics. The TGDC recommends that the ICDR consider the topic of voting system accessibility for one of ICDR's annual conferences.

Ms. Quesenbery offered context on the resolution." The ICDR is the interagency committee on disability research and their role in the federal government is to facilitate interagency research on topics of interest to the disabilities community. They actively seek input from stakeholders on topics for research they can fund to bring together research communities that might not have met otherwise." She noted that the U.S. Access Board felt that a resolution of endorsement from the TGDC would be helpful in moving forward.

The Chair asked for a second to the motion.

The motion was seconded.

There being no discussion, the Chair asked for unanimous consent to adopt the resolution. Resolution 08-06 was adopted by unanimous consent. (See Table 1.)

The Chair recognized Mr. Berger. He offered Resolution 09-06 for consideration by the Committee.

Resolution 09-06 Title: Principal Criteria
Offered by Mr. Stephen Berger

To be certified to the standard, a voting system must be:

- *Secure*
- *Accurate*
- *Reliable*
- *Usable*
- *Accessible*
- *Fit for its intended use.*

All other requirements of this standard are established to define these requirements more clearly, apply them to specific voting system technologies, and make them more objectively testable. However, in case of conflict, these principal criteria take precedence. Hence, if a candidate's voting system demonstrably is not secure, accurate, reliable, usable, accessible, or fit for use, it shall be judged to fail the criteria of these guidelines.

Dr. Rivest expressed his concerns. "If there is an egregious security problem, of course, the system should fail, and I would hope that the guidelines would cause that to happen. The advantage of clear, precise, testable requirements, to the extent that you can get them, is that you avoid some of these issues of judgment that come up."

Dr. Williams expressed his support for the resolution. "I think what we are trying to do here is recognize that no matter how hard we try, we might leave things out of these standards. If a vendor comes in for testing with a voting system, and he has found a path to technically comply with the standard, yet it is obvious that the system doesn't satisfy one of these fundamental criteria, this resolution would give us a reason for turning down acceptance of the voting system. Without this resolution, if the system meets all the individual requirements, you have no recourse but to approve it in accordance with the conformance clause."

In answer to Committee questions as to how this resolution would be implemented, Mr. Berger summarized the process. First, the test engineer at the voting system test laboratory would conclude that there is a failure of sufficient weight that they could not professionally recommend accreditation or certification. It would stop there unless the vendor then wanted to appeal that decision to the EAC. In that instance, the EAC would likely have their technical experts review the decision for appropriateness. The EAC technical expert and the laboratory testing engineer would both need to recommend to the EAC that, in fact, even though in some manner this system passed all the specific written tests, there was a flaw of sufficient weight that the system should not be certified."

Ms. Quesenbery questioned whether this resolution did not deal with the certification process. "The resolution sounds to me like a judgment call that you would want to have presented to the EAC from the certification process rather than something that should be written into the requirements."

After considerable discussion, the Committee agreed on the high-level goals of the resolution. Mr. Berger accepted several friendly amendments to the wording.

Resolution 09-06 (As Amended) Title: Principal Criteria
Offered by Mr. Stephen Berger

The TGDC will include in the guidelines as a statement of the overall goal to produce systems
with the following attributes:

- *Secure*
- *Accurate*
- *Reliable*
- *Usable*
- *Accessible*
- *Fit for its intended use*

This may allow for the certifying authority to consider whether a candidate's voting system not only is in conformance with the requirements, but also whether it meets the higher-level goals.

The Chair asked for a second to the resolution as amended. The motion was seconded. Dr. Jeffrey asked if there was objection to unanimous consent for the resolution as amended. There was none. Resolution 09-06 was adopted by unanimous consent.

Mr. Berger offered his final resolution for consideration.

Resolution 10-06: Title: Reliability Metrics
Offered by Mr. Stephen Berger

The TGDC concurs with moving away from MTBF (Mean Time Between Failure) as a reliability metric for voting systems.

Mr. Berger offered context to this resolution. "In light of yesterday's discussions during the core requirements discussion, I recommend moving reliability metrics away from

Mean Time Between Failure (MTBF) towards a probability of failure during an election metric. I think clearly we are interested in the chance that equipment will fail during an election."

Ms. Quesenbery asked whether such a resolution was necessary since the TGDC had accepted the preliminary core requirements report delivered by Dr. Flater yesterday.

Dr. Flater offered his understanding of the Committee's guidance. "Given the probability of failure as one of the inputs, we would then calculate reliability benchmarks to ensure that the probability of failure in an election would be less than that."

There being no further comment, the Chair asked for a second to the resolution. The motion was seconded. Without objection, Resolution 10-06 was adopted by unanimous consent. (See Table 1.)

Dr. Rivest asked to make a point of clarification. "I want to just revisit quickly a topic that Nelson Hastings had addressed earlier and to just make it clearer where the STS subcommittee is going in one area. We talked about cryptographic modules. I just wanted to make it clear to my colleagues on the Committee that it is the plan of the STS to push for requirements that make hardware cryptographic modules mandatory in future voting systems so that they can authenticate the communications between various modules. This is a hardware requirement and as such, I think it is significant. I look forward to discussions both within STS and the joint meetings between STS and CRT subcommittees, or any other form that the Committee members like. I think it is has a lot of benefits."

At the recommendation of Committee members, Dr. Jeffrey formally asked for approval of the STS preliminary reports. "The Security and Transparency Subcommittee has provided a preliminary report that responds to eleven different TGDC resolutions that have been previously adopted. Unless there is additional direction, given the resolutions and given the feedback that NIST staff has received during this meeting, they will then continue to develop their guidelines consistent with the path that they had outlined, moderated by the resolutions and the discussions.
Are there any further questions or issues?"

There being no further discussion, the Chair asked for a second. The motion was seconded. The Chair asked for approval by unanimous consent. There was no objection. The STS preliminary report was adopted by unanimous consent. (See Table 1.)

The Committee then reviewed potential dates for the next TGDC meeting in the March 2007 time frame. Members agreed to provide Mr. Eustis with their preferences for a two day meeting.

The Chair thanked NIST staff and the Committee for their hard work. Dr. Jeffrey then adjourned the meeting.