# Four Approaches to SI and Accessibility

Prepared at the direction of the HFP and STS Subcommittees of the TGDC

March 12, 2007

This paper has been prepared by the National Institute of Standards and Technology at the direction of the HFP and STS subcommittees of the Technical Guidelines Development Committee (TGDC). It may represent preliminary research findings and does not necessarily represent any policy positions of NIST or the TGDC.

The Technical Guidelines Development Committee is an advisory group to the Election Assistance Commission (EAC), which produces Voluntary Voting System Guidelines (VVSG). Both the TGDC and EAC were established by the Help America Vote Act of 2002. NIST serves as a technical adviser to the TGDC.

# 1. Introduction

On Dec 5, 2006, the TGDC unanimously adopted resolution #06-06, stating that:

> ... 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**...

Thus, in the future, only software-independent (SI) voting systems will be eligible for certification. An SI system is defined as one in which **"a previously undetected change or error in its software cannot cause an undetectable change or error in an election outcome."** That is, even if the software fails or is incorrect, there is still a mechanism which would allow such detection. Examples of such systems include DRE + voter-verifiable paper audit trail (DRE/VVPAT) systems and systems with paper ballots. It may in the future include other more advanced paperless designs, such as "witness" and "frog" systems. A counterexample is, of course, the simple DRE system.

The TGDC resolution assumes that SI will be achieved through the specific mechanism of voter verification of the voting record, even though it might be argued that other means exist.

HAVA 301(A) (3)(a) describes an accessible system as follows:

> "Accessibility for individuals with disabilities.--The voting system shall--
>
> 1. be accessible for individuals with disabilities, including nonvisual accessibility for the blind and visually impaired, in a manner that provides the same opportunity for access and participation (including privacy and independence) as for other voters;"

The purpose of this paper is to explore how both these goals, SI and accessibility, can be achieved.

# 2. Methodology of Analysis

We consider four implementations which motivate our discussion. Our analysis examines four criteria: 1) degree of SI and of independent dual verification (IDV), 2) voter verification of the independent record (VV), 3) accessibility and also general usability, and 4) usability of auditability. The accessibility criterion will focus on the problems of voters with poor vision, but dexterity can also be relevant. We evaluate only those problems that seem inherent to the approach itself, not additional problems that might be introduced by poor implementations.

## 2.1 Feasibility

We do not take into account feasibility of implementation, since the purpose is to decide what might constitute a *sufficient technique.* That is, if it turns out that approach X has good properties for SI , accessibility of VV, and auditability, the result would be a requirement stating that X may be used to satisfy these goals, not that X is required for all implementations. Of the four approaches discussed below, only the first is currently available as a mainstream commercial product.

## 2.2 SI, IDV, VV

Perhaps the most basic premise of voting security is not to place all our trust in a single automated system. Three terms are commonly used to describe ways in which we check up on the "primary" system. The precise definitions below are critical to our analysis.

**Software independence (SI)** is a global property of the system, namely that no purely technological problem can go undetected in the election as a whole. That detection might occur as a direct result of voters' observations, or during a subsequent audit. But, by definition, no system that relies entirely on technology can be SI. Some human-performed checking is a necessary condition. In this analysis, SI implies security independent of all technology. However, we also explore the possibility of security that is independent of the "primary" voting system, but may rely on smaller and simpler secondary assistive technology devices.

**Independent Dual Verification (IDV)** is a slightly less stringent condition. It requires that a second "independent" system (whether automated or human) be used to check on the first. Thus, purely automated solutions are possible, accepting the risk that the two systems might not really be independent or might otherwise mask failure.

**Voter Verification (VV)** is the capability of *individual* voters to verify a record of their ballot choices. Two properties of that record have been up for discussion: its *independence* and its *permanence*. The TGDC resolution refers to an "independent" record; "permanent" is usually understood to imply non-electronic. VV has two roles: 1) as one way (among others) for achieving SI and 2) as a way of building confidence for individual voters. We make a distinction between what some call "verification" but is merely the summary or confirmation screen on the DRE which can be visual or audio. This is NOT considered voter verification in our analysis because it is not a verification of the independent, permanent record. For an analysis of different voter verification scenarios for blind and sighted voters, see the Appendix at the end of this paper.

### *2.3 Observational Testing Defense*

We now introduce a notion of how one can ensure some degree of trust in an accessible voting station and also preserve the SI of the voting system. This procedural defense, which we call **observational testing,** is a way to ensure that the accessible, audio voting station can be trusted to be SI. We describe the concept in terms of an audio/visual screen with a paper record. A few voting officials and volunteers are asked to use the audio interface to vote, and are asked to note any problems. They must check the screen, the audio, and the paper record. If they notice a disagreement between the paper record and electronic record, they should do the normal process of complaining about the machine and rejecting the paper record. However, they should also report their problems to the state election authorities. This simple defense is very likely to detect a compromised accessible voting station. It also has the added desirable property of preserving privacy by increasing the number and type of voters using the station.

In order to avoid detection, the attacker must either attempt to distinguish between voters with vision problems and voters with good vision or must try to apply the attack for only a small fraction of voters using the audio ballot, and hope that very few or none of the other voters happen to trigger the attack. This is somewhat like parallel testing, but far harder for the tampered software to detect, because it is only happening for a single vote at a time, and it does not require isolating the voting station. Because audio ballots are only a small minority of all ballots cast, someone trying to change an election outcome using this attack cannot afford to exclude many audio ballots from its attack.

### *2.4 Scope*

There is no intent to preclude the consideration of approaches beyond the four listed below. Further, our examination of these approaches focuses primarily on their use by people with disabilities in keeping with the TGDC resolution #6-06 and the HAVA mandate to ensure people with disabilities can vote independently and privately while also preserving SI.

## 3. Descriptions of Technical Approaches

This section describes the four approaches we considered and the steps for using them. A summary table at the end of this document shows the steps for all four systems side by side.

### *3.1 Audio review-only with observational testing*

In this approach, vision-limited voters hear a confirmation (the audio of the summary screen) of how they voted and a paper record is also generated, but the paper itself is not necessarily examined. Examples include DRE+VVPAT and electronic ballots markers and printers. The process is:

Step 1: Voter marks ballot using electronic system, which prints ballot (or paper audit trail) and the accessible voting station provides audio of the ballot marking and review process.

Step 2- alternative A: Sighted voter (sometimes) verifies printed paper ballot.

Step 2 - alternative B: Blind, low vision, low literacy, second language, or non-written language voter: No action on the part of the voter, because the paper audit trail is not accessible.

Step 3: Voter casts the ballot.

Audit: Auditing relies on paper ballots only.

The system is SI because observational testing ensures that the accessible system can be trusted and because SI is a global property and does not require every voter to verify. However, voters using alternative B in Step 2 cannot directly verify their paper records. The accuracy of the electronic record is assumed through the use of observational testing.

## *3.2 Audio Recording*

This is the same as Audio review-only, except that a recording of the audio confirmation is made and preserved. The tape (or digital file) serves as a permanent verified record, closely analogous to the role of paper for sighted voters. The process is:

Step 1: Voter marks ballot using electronic system, which makes an audio recording of the review, and which prints ballot (or paper audit trail).

Step 2-alternative A: Sighted voter (sometimes) verifies printed paper ballot.

Step 2-alternative B: Blind, low vision, low literacy, second language, non-written language voter skips this step (audio recording serves as their permanent record).

Step 3: Voter casts ballot.

Audit: Auditing relies primarily on paper, can use audio records if there is a problem.

Note that this system design assumes that the audio recording is an independent, permanent record. A voter who is blind must trust that the system is indeed recording the audio as it is being heard and not generating an altered audio record. It may be difficult to ensure that indeed it is an authentic record that has not been altered in some way, e.g., digitally. There are also usability problems in handling multiple cassette tapes. In addition, it is time-consuming to listen to audio tapes.

## 3.3 Audio plus Scanning the Paper Record with observational testing

In the previous two approaches, paper is generated as somewhat of a byproduct for DRE-VVPAT systems. In this approach, the paper itself (the optical scan ballot or the paper audit trail) is scanned directly, e.g. with optical character recognition (OCR), and an audio version is generated for the voter to verify. Note the similarity to the Frog System (following): in both, a record is generated by the primary system and then read by a second, more trusted system. The process is:

> Step 1: Voter marks ballot using electronic system, which prints ballot (or paper audit trail).
>
> Step 2 alternative A: Sighted voter (sometimes) verifies printed paper ballot.
>
> Step 2 alternative B: Blind, low vision, low literacy, second language, non-written language voter (sometimes) uses device that "reads back" the ballot for verification using OCR. A barcode reader is another possibility, to trust that the barcode is an accurate record means an extra step for observational testing.
>
> (Note that for VVPAT, the paper audit trail is read back; for electronic ballot markers, the printed ballot is read back and then submitted to the precinct counter optical scanner or PCOS for casting. An interesting proposal is that the PCOS itself could have a trusted audio OCR that the voter can request when the ballot is submitted.)
>
> Step 3: Voter transports ballot to PCOS device, inserts and scans ballot to cast.
>
> Audit: Auditing relies on paper ballots only.

## 3.4 Frog Systems

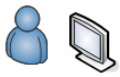
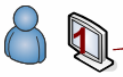
Certain systems have been proposed that would provide paperless verification. (We do not include *visual* witness systems for consideration, since voters with poor vision cannot examine the display screen in the first place.) A so-called "frog" system is one in which an electronic record of the ballot is transmitted to a second trusted system which echoes it back (visually or aurally) to the voter. Note that this system is not SI. The process is:

> Step 1: Voter marks ballot using electronic system.
>
> Step 2: Second system presents review (using same output – visual or audio – used in Step 1.
>
> Step 3: Voter casts ballot.
>
> Audit: Auditing relies on trusted second system.

## *3.5 Summary tables for the four approaches*

For side-by-side comparison, we summarize the steps in the voting process for each of the approaches with a visual table (followed by the text version of the table.)

### *Summary of the voting process of the four approaches (visual version)*

| | Step 1<br>Voter marks the ballot | [ Independent voting record created ] | Step 2<br>Voter verifies record | Step 3<br>Voter casts ballot |
|---|---|---|---|---|
| 1<br>AUDIO REVIEW + OBSERVATION TESTING |  <br>Voters mark ballot using either the visual or audio interface. The final step of ballot marking is a review screen. |  <br>Paper audit trail created |  **A: Sighted voters:** Verify the printed record<br>  **B: Blind, low vision, low literacy, 2nd language, non-written language:** No action |  <br>Voters cast ballot on the electronic device<br>Audit uses printed record |
| 2<br>AUDIO RECORDING |  <br>Voters mark ballot using either the visual or audio interface. The final step of ballot marking is a review screen. |  <br>Paper audit trail created when visual interface is used.<br>**OR**<br>  <br>Audio of review screen recorded when audio interface is used. |  **A: Sighted voters:** Verify the printed record<br>  **B: Blind, low vision, low literacy, 2nd language, non-written language:** No additional action<br>Audio recording serves as their permanent record |  <br>Voters cast ballot on the electronic device<br>Audit uses printed record or audio record. |
| 3<br>AUDIO + SCANNED PAPER RECORD |  <br>Voters mark ballot using either the visual or audio interface. The final step of ballot marking is a review screen. |  <br>Printed ballot created<br>**OR**<br>  <br>Paper audit trail created |  **A: Sighted voters:** Verify the printed ballot or audit trail<br>  **B: Blind, low vision, low literacy, 2nd language, non-written language:** Second device used for OCR and then to "read back" the ballot or audit trail |  **PRINTED BALLOT:** Voters cast ballot on PCOS device<br>**OR**<br>**VVPAT:** Voters cast ballot on the electronic device<br>Audit uses printed record |
| 4<br>FROG SYSTEM |  <br>Voters mark ballot using either the visual or audio interface. The final step of ballot marking is a review screen. | A copy of the record is transmitted to a second system |  <br>Second system presents review (using same output – visual or audio – used in Step 1) |  <br>Voters cast ballot on the electronic device<br>Audit relies on second trusted system |

This paper has been prepared at the direction of the HFP and STS subcommittees. It does not necessarily represent any policy positions of NIST or the TGDC.

## *Summary of the voting process of the four approaches (text version)*

| | **Step 1**<br>**Voter marks the ballot** | **Independent voting record created** | **Step 2**<br>**Voter verifies record** | **Step 3**<br>**Voter casts ballot** |
|---|---|---|---|---|
| **1. Audio Review Only** | Voters mark ballot using either the visual or audio interface. The final step of ballot marking is a review screen. | Paper audit trail created | **A: Sighted voters:** Verify the printed record<br><br>**B: Blind, low vision, low literacy, 2nd language, non-written language:** No action | Voters cast ballot on the electronic device<br><br>Audit uses printed record |
| **2. Audio Recording** | Voters mark ballot using either the visual or audio interface. The final step of ballot marking is a review screen. | Paper audit trail created when visual interface is used.<br><br>OR<br><br>Audio of review screen recorded when audio interface is used. | **A: Sighted voters:** Verify the printed record<br><br>**B: Blind, low vision, low literacy, 2nd language, non-written language:** No additional action<br>Audio recording serves as their permanent record | Voters cast ballot on the electronic device<br><br>Audit uses printed record |
| **3. Audio + Scanned Paper** | Voters mark ballot using either the visual or audio interface. The final step of ballot marking is a review screen. | Printed ballot created<br><br>OR<br><br>Paper audit trail created | **A: Sighted voters:** Verify the printed ballot or audit trail<br><br>**B: Blind, low vision, low literacy, 2nd language, non-written language:** Second device used for OCR and then to "read back" the ballot or audit trail | **PRINTED BALLOT:** Voters cast ballot on PCOS device<br><br>OR<br><br>**VVPAT:** Voters cast ballot on the electronic device<br><br>Audit uses printed record |
| **4. Frog System** | Voters mark ballot using either the visual or audio interface. The final step of ballot marking is a review screen. | A copy of the record is transmitted to a second system | Second system presents review (using same output – visual or audio – used in Step 1) | Voters cast ballot on the electronic device<br><br>Audit relies on second trusted system |

This paper has been prepared at the direction of the HFP and STS subcommittees. It does not necessarily represent any policy positions of NIST or the TGDC.

## 4. Analysis

This table summarizes how the four systems meet the criteria outlined. Analysis notes follow the table.

| **System Type** | **SI** (trustworthiness of ballots cast) | **VV** (verifiability for voters with disabilities) | **Accessibility / Usability** (for voters with disabilities) | **Auditability** (usability for election officials) |
|---|---|---|---|---|
| Audio-review-only | √<br>SI | –<br>Not VV | √<br>Good Access<br>Good Usability | √*<br>* Assumes high quality paper record |
| Audio Recording | √<br>SI | √<br>Alternate permanent record for Acc-VS | √ –*<br>Good Access<br>*Usability? See analysis notes | –<br>Poor. |
| Audio plus Scanning Paper | √*<br>SI<br>* Must trust the "reader" that translates the paper into audio. | √<br>VV<br>Voters offered alternate means to verify their ballot | √ –*<br>Good Access for blind, low vision.<br>* Reduced independence for dexterity.<br>*Weak Usability | √*<br>* Assumes high quality paper record |
| Frog System | –<br>Not SI<br>Possibly IDV | –<br>Not direct VV | √<br>Good access<br>Usability depends on ease of comparisons. | √<br>Audit usability good. No paper required. |

## *Analysis notes*

**Audio-review-only**

- SI assumes that the sighted voters using the Acc-VS would notice discrepancies between the audio and paper.
- This approach is not VV because blind/low vision voters cannot verify the permanent paper record.
- Good accessibility and usability - no "extra" steps required of voter.
- Assuming high quality paper record, this approach provides good auditability, however some noted that paper can be difficult to count.

**Audio recording**

- This approach is not only SI, but provides an alternate permanent record for voters who cannot verify paper. It assumes that the tapes are monitored by humans in the audit.
- It is VV because an alternate permanent record for Acc-VS
- It has good accessibility because the verification step is transparent and there is no handling of the paper record required.
- In principle, the usability for the voter should be good—the tape should automatically and transparently capture the audio. However, the handling of tapes for both the voter and poll workers could be quite complex. Since only a prototype has demonstrated this approach, it is difficult to determine usability.
- For auditability, there are usability issues based on difficulties in handling tapes for election officials. No current procedures for conducting an audit of an audio record. This audit can be time-consuming if manual or relies on voice recognition technology.

**Audio plus Scanning Paper**

- This approach is SI, but voters must trust the "reader" that translates the paper into audio. Also, this inherits the "barcode" issue: there are now *four* copies of the ballot (electronic, paper/text, paper/barcode, audio) to co-ordinate. OCR eliminates at least the "opaque" paper record.
- Voters are offered alternate means to verify their ballot. This approach provides good access for blind, low vision, but reduces independence for voters with dexterity disabilities. It also assumes a method of transporting ballot privately.
- Usability is weaker because of the extra steps required for a low vision or low literacy voter to complete the verification.
- Assuming high quality paper record, this approach provides good auditability, however some noted that paper can be difficult to count.

**Frog System**

- Possibly IDV, not SI, depending on whether the second system is truly independent and trustworthy.

- This approach does not offer direct verification because no permanent (non-electronic) record is generated.
- It has good accessibility because there is no handling of the paper record required, and voters with disabilities use the same process as other voters.
- Usability depends on ease of comparisons.
- Audit usability should be very good. No paper required.

## *Appendix: Analysis of Scenarios for Voter Verification*

As part of the analysis of voter verification, we found it helpful to compare the characteristics of voter verification for a range of voter scenarios. This table looks at the communication technology used, without regard to any specific approach.

The main point here is that it is quite difficult to put the blind voter in the same epistemic position as the sighted voter. The sighted voter both sees the contents of the paper record *and that there is a paper record with those contents.* This is not unique to paper. A voter using Braille has analogous assurance, however, this is not a universal solution as many people with low vision or recently blind do not read Braille.

But how would we get past that "not easily" entry in the table? For the purposes of the argument, one thinks of a scenario like this: the voter brings her own (trusted) tape player. The voting system produces a tape cassette with her ballot choices. She handles the cassette, puts it in her player, and verifies the contents. Now she knows that the record exists.

This table points out the dilemma of how to address what it means to provide voter verification for voters who are blind.

### *Comparing Voter Verification Characteristics for Blind and Sighted Voters*

| Scenario | Can voter verify contents? | Does independent record exist? | Can voter verify existence of record? |
|---|---|---|---|
| Sighted voter + screen | Yes | No | No |
| Blind voter + generated audio | Yes | No | No |
| Sighted voter + paper | Yes | Yes | Yes |
| Blind voter + Braille | Yes | Yes | Yes |
| Blind voter + audio record | Yes | Yes | Not easily |