Technical Guidelines Development Committee
March 22, 2007, Plenary Meeting

Equipment Requirements to Support Auditing Steps

Presentation for the
Technical Guidelines Development Committee (TGDC)

March 22/23, 2007

Introduction

- Some threats to voting systems can only be addressed through procedural defenses
  - Software independence requires auditing procedures
- VVSG is equipment standard
- VVSG will require equipment to ***support*** critical auditing steps
  - Equipment, documentation, testing
- At high level, these apply to innovation class
  - But details depend on how those systems work

What Threats are We Addressing?

- Voting Machine can:
  - Change recorded votes
    - Defense: Hand Audit, Observational Testing
  - Give wrong ballots
    - Defense: Pollbook Audit
  - Introduce errors favoring one side
    - Defense: Parallel Testing, Spot Parallel Testing
- Tabulation Center Computer can:
  - Miscount votes
  - Omit or insert machine totals
    - Defense: Reconciling Machine/Precinct/Final Totals

Auditing Steps to be Supported

- Verifying agreement between records
  - Pollbook audit
  - Hand audit
  - Final tally audit
- Verifying presentation and machine
  - Observational testing
  - Parallel testing/ Spot parallel testing

Making Sure Records Agree

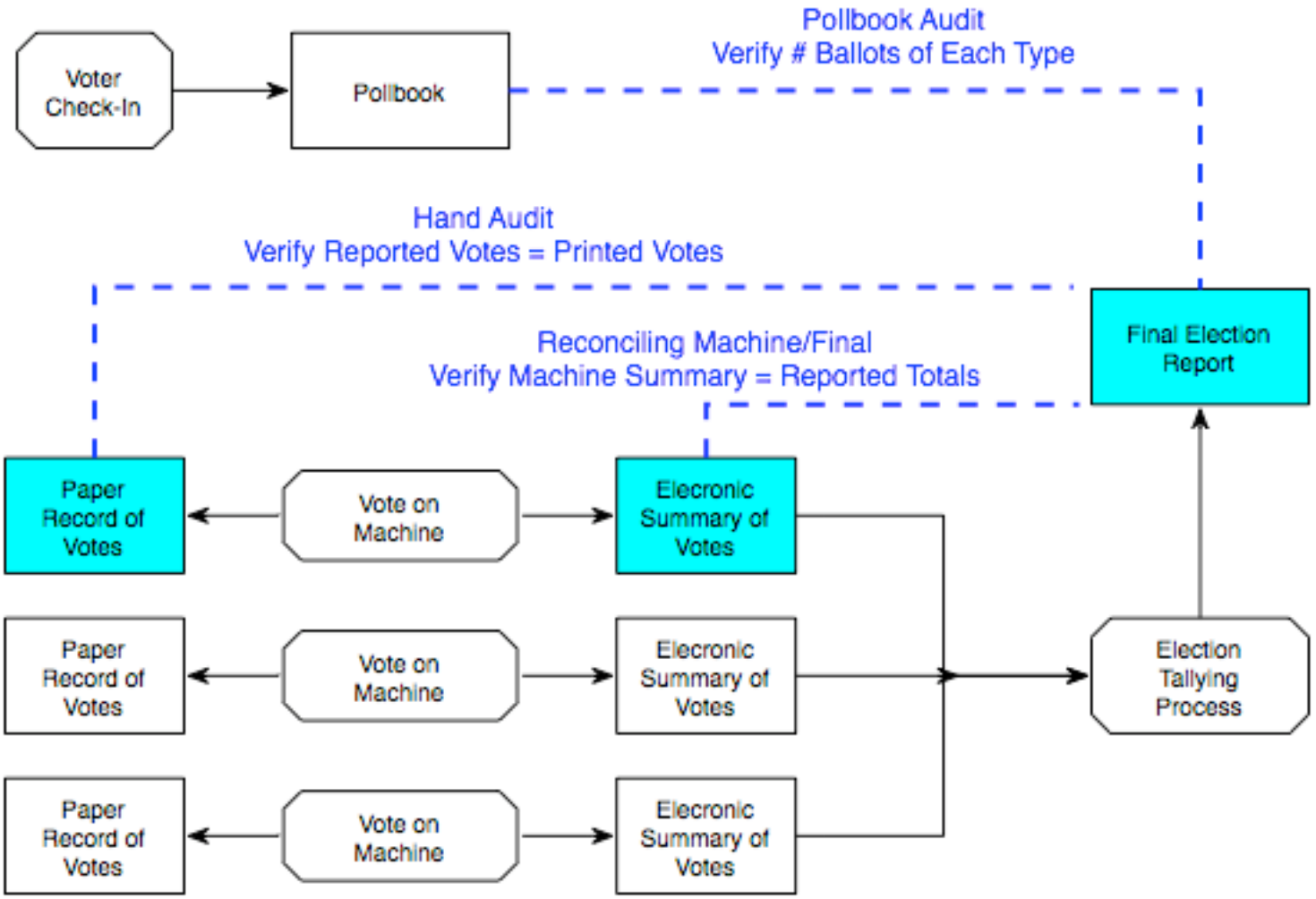
- Many attacks leave some disagreement between records--auditing steps detect this
- Current practice already include auditing
- Goal:
  - Strengthen current mechanisms

- *Requirements are about what must appear:*
  - *What must appear in VVPR,*
  - *in summary from voting machine, and*
  - *in final election report.*

Paper and Electronic Records

- VVPR = paper record voter can verify
  - VVPAT or paper ballots (hand- or machine-marked)
- Machine summary
  - Electronic summary of votes per machine
  - Signed, printable
- CVRs = cast vote records
- Final Election Report
  - Full report of election result,
  - Breakdowns by precinct/polling place/machine.

Technical Guidelines Development Committee
March 22, 2007, Plenary Meeting

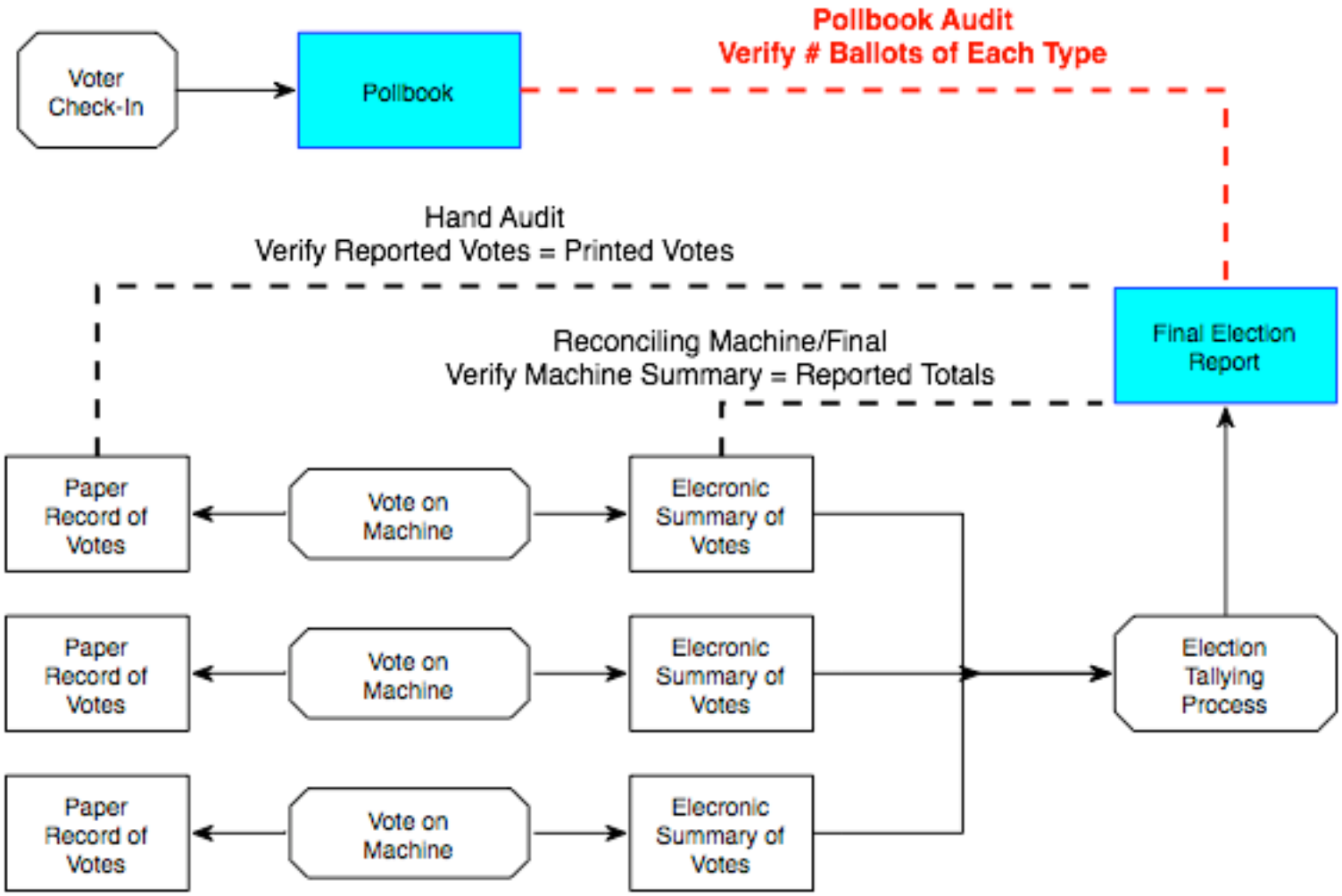


Pollbook Audit

Verify number of voters for each ballot type equals number of that ballot type recorded

- Threats:
  - Added/deleted votes
  - Silent "redistricting" by voting machines
- Requirements:
  - Machine summary contains breakdown by ballot type (ballot style, election district, precinct)
  - VVPRs identify ballot type of each voter
  - Final Tally Report contains breakdown by ballot type for each polling place / machine

Technical Guidelines Development Committee
March 22, 2007, Plenary Meeting

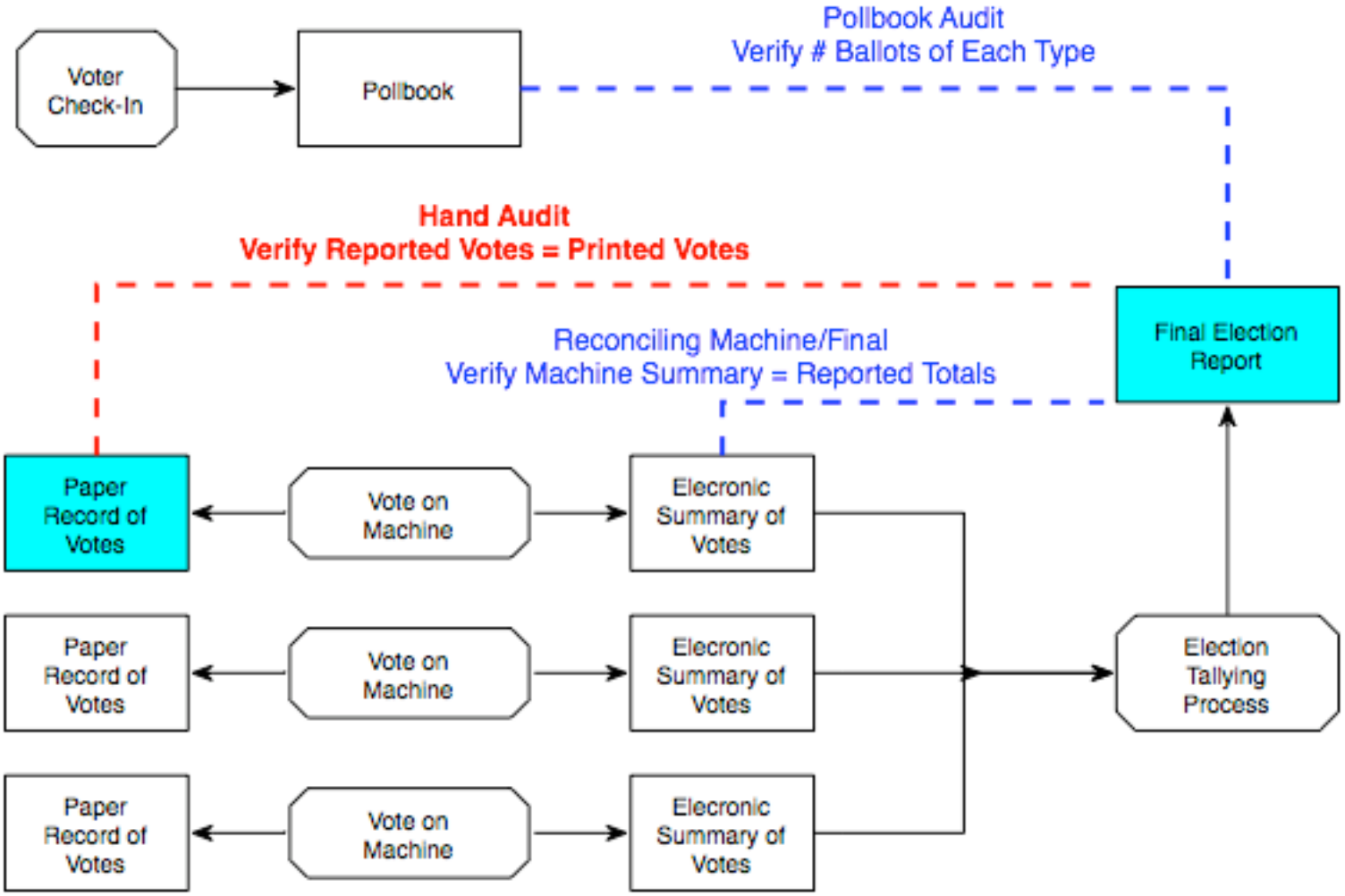


Hand Audit

Verify agreement between paper records voters could see and recorded results.

- Threats:
  - Voting machine silently changing recorded votes
- Requirements
  - VVPRs:
    - Each ballot or ballot record includes ballot type, all information needed to count
    - Provisionals and write-ins clearly marked
  - Final Election Report
    - Results broken down by precinct, polling place, and machine

Technical Guidelines Development Committee
March 22, 2007, Plenary Meeting

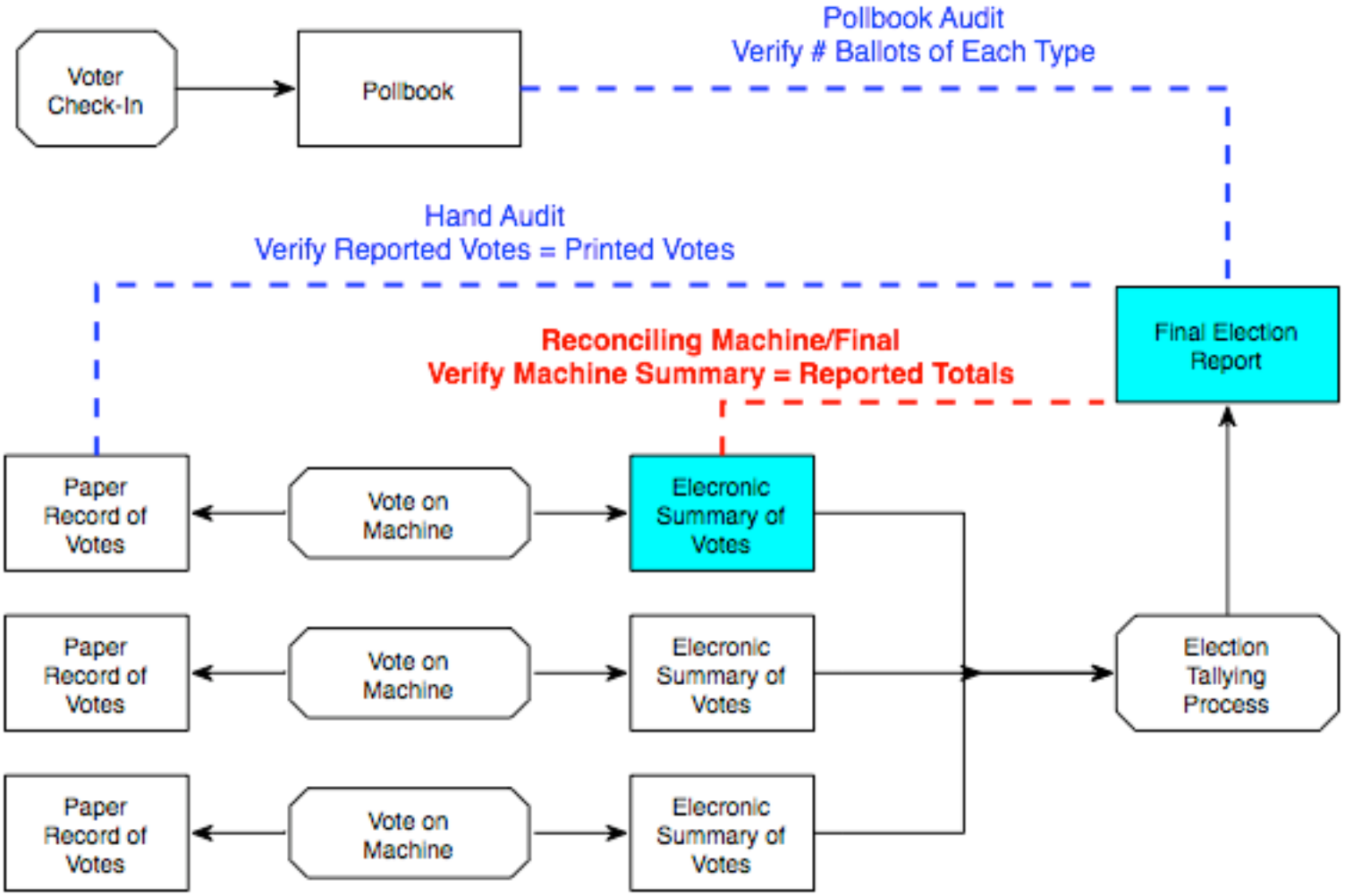


Reconciling Totals

Verify machine totals included correctly in final total.

- Final Election Report able to include:
  - Totals for each machine (correspond to summary records)
  - Total # ballots, # of each type for each machine and polling place
  - Handle provisionals/write ins
    - Batch in summaries per precinct or polling place
    - Include in final totals
- Summary Record
  - Totals for each ballot question, and total # ballots

Technical Guidelines Development Committee
March 22, 2007, Plenary Meeting



Summary of Procedures to Check Agreement of Records

- Strengthen existing procedures
  - Include all data needed for efficient auditing steps
  - Include digital signatures on electronic records
  - Requirements should have little impact on cost or operation of voting equipment

Auditing Steps to be Supported

- Verifying agreement between records
  - Pollbook audit
  - Hand audit
  - Final tally audit
- **Verifying presentation and machine**
  - **Observational testing**
  - **Parallel testing/ Spot parallel testing**

Presentation and Machine Behavior

- Even with VVPR, machines can misbehave
  - Indicate vote for X, print/record vote for Y
  - Introduce "errors" favoring one candidate
  - Skip some ballot questions
  - Present ballot in confusing/incorrect way

These threats are easier to detect

- Voters have a chance to catch misbehavior
  - Many voters will notice "accidental" error and fix it on summary screen
  - Voters may complain
- Still may have an effect on outcome
- EXCEPT for blind/alternative language voters
  - Need additional defense

Audit Procedures

- Goal: Detect misbehavior during voting process, on election day
- Audit Procedures:
  - Observational testing
  - Parallel testing
  - Spot parallel testing
- How much experience do we have?
  - Some states have done parallel testing
  - All states do testing before election

Observational Testing

Ensure that VVPATs and ballot markers correctly print ballots/summaries for users of audio ballots.

- Threat: Voting machine could print and record wrong vote whenever voter used audio ballot.
- Procedure: Have small number of authorized voters volunteer to:
  - Use audio ballot interface
  - Verify correctness of printed record
- Requirements:
  - Tokens/numbers to authorize voters must not allow machine to distinguish blind/sighted voters

Parallel Testing

Verify correct behavior of voting system on election day, under normal voting conditions.

- Threats: Voting machine could introduce differential errors, silently misrecord/misprint occasional votes
- Requirements: VVPAT required to support parallel testing

Supporting Parallel Testing

- Must be possible to isolate voting machine
  - No contact with anything outside of testing team's control.
- Voting machine must not detect isolation
  - If it can detect testing, it can evade test
- Voting machine must commit to results before connecting outside testing team.
  - Otherwise, could change results at end.

These are potentially expensive to support

- Isolation means no networking outside set of machines to be tested
  - Maybe test a whole network of machines?
  - Requires testers bringing in/setting up new network!
- Imposes requirements on authenticating voter to machine

Spot Parallel Testing

- Much easier to do for ballot markers with no memory
  - Tester can cast test ballot, verify correct results printed.
  - Parallel test for only one vote instead of machine for whole day.
- Requirements on authentication mechanism for voters
  - Don’t permit signaling to ballot marker.

Summary of Procedures to Address Presentation Attacks

- Observational testing is straightforward and powerful
- Spot parallel testing seems workable
- Parallel testing is very expensive
  - Require equipment to support
  - Not sure how many states will use

Technical Guidelines Development Committee
March 22, 2007, Plenary Meeting

Discussion