

# Public Transparency Protocol (PTP) Procedures

Draft by Raymond Lutz, Citizens Oversight -- 4/27/2026 REF: [M2053](#)

## Introduction

This document is submitted as a technical companion to the accompanying comment on *Voluntary National Principles for Election Auditing and Testing – A Practical Guide*. The comment document recommends the adoption of Public Transparency Protocols (PTPs) as an essential operational mechanism for ensuring verifiability in election auditing and testing processes.

The material presented here provides an initial draft set of PTP procedures to illustrate how those principles can be implemented in practice. These procedures are not proposed as final standards, but as concrete, repeatable patterns that demonstrate how key activities—such as logic and accuracy testing, batch comparison audits, risk-limiting audits, ballot accounting, and system integrity checks—can be conducted in a manner that enables real-time public observation, verification, and complete documentation.

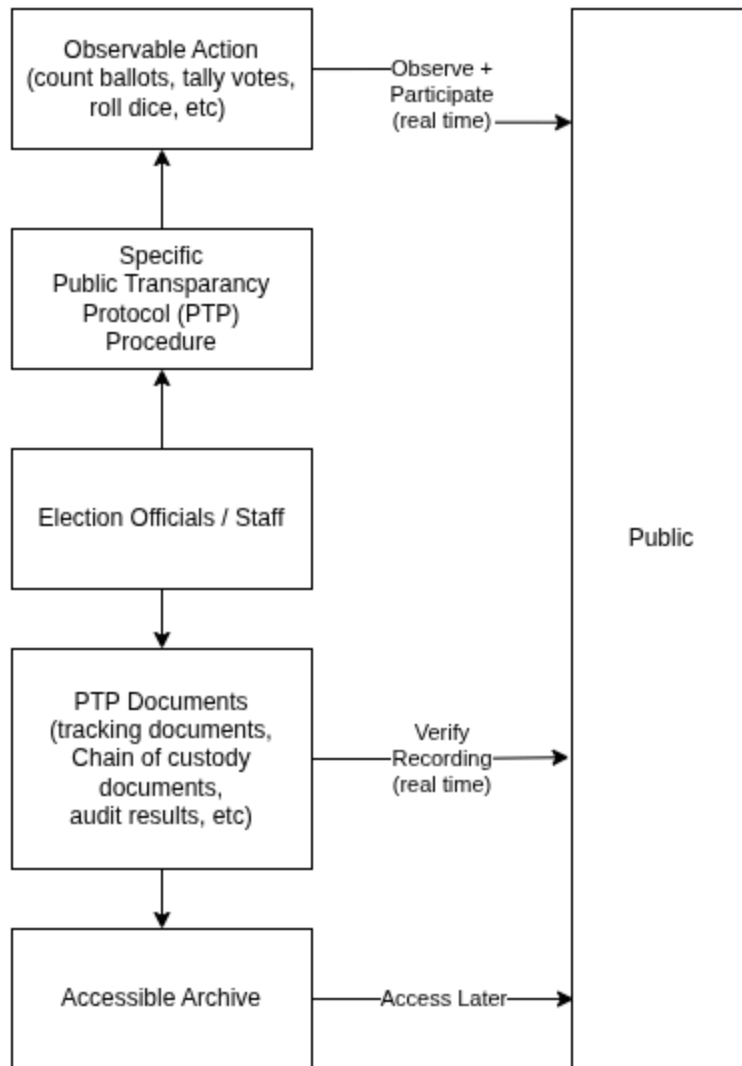
The intent is to show that the concepts described in the comment document are operationally feasible, can be consistently structured across different processes, and may serve as a foundation for future development of standardized audit and testing protocols.

## PTP Framework (applies to all procedures)

All PTP procedures follow these invariants:

- **Real-time visibility:** all actions and all recording occur in view of observers and also to be webcast.
- **No hidden steps:** there is no off-camera/off-record staging.
- **Complete records:** intermediate values and repeated measurements are preserved.
- **Structured recording:** values are captured in human-readable and machine-readable fields on a PTP sheet.
- **Verification points:** observers can confirm that recorded values match observed values at the moment of entry.
- **Artifacts:** each procedure produces one or more PTP sheets (with unique IDs) suitable for scanning and later analysis.

# Public Transparency Protocol (PTP) Framework



# 1. Batch Comparison Audit (one PTP sheet per batch)

## Purpose

Compare reported totals for a batch (precinct/container) to a manual tally or independent system output.

## Inputs

Batch identifier, reported totals by contest, ballots in sealed container.

## Procedure

1. **Present batch:** display batch ID, seal IDs, and storage location in view of observers.
2. **Verify seals:** read and record seal numbers; observers confirm they match logs.
3. **Open container:** break seal in view; record time and personnel.
4. **Count ballots (pass 1):** perform manual count; record count.
5. **Count ballots (pass 2):** repeat; record second count. If mismatch, perform additional counts; **record all attempts.**
6. **Tally by contest:** perform manual tally (or independent tabulation) for all contests on the batch; record results.
7. **Record reported totals:** transcribe official reported totals for the same batch.
8. **Compare:** compute differences; record per-contest variances.
9. **Resolve discrepancies:** if differences exist, re-tally; record each re-tally and outcome.
10. **Reseal:** return ballots; apply new seal; record new seal ID.

## Recording (PTP Sheet)

Header (date, location, batch ID, seal IDs, staff), ballot counts (all passes), per-contest tallies (manual and reported), differences, notes, new seal ID, sheet ID (QR).

## Public verification

Observers witness seal verification, all counts, all entries on the sheet, and the comparison results as written. Observers can independently recompute differences from visible values.

---

# 2. Risk-Limiting Audit (RLA) PTP (card-level with ARLO or CORLA-style systems)

## Purpose

Select and examine a random sample of ballot cards and evaluate outcomes using RLA methods.

## Inputs

Contest definition, risk limit, ballot manifest, RNG method, audit system (e.g., ARLO/CORLA).

## Procedure

1. **Define parameters:** display contest, risk limit, and audit settings; record.
2. **Generate randomness:** produce seed via public method (e.g., dice); record each roll; compute seed; observers verify calculation. (This can be a separate PTP)
3. **Initialize system:** enter parameters and seed into audit system; screen is visible; record inputs.
4. **Select sample:** generate sample list; display IDs; record selection on PTP sheet.
5. **Retrieve ballots:** locate each selected ballot using manifest; verify container and position; record retrieval details. Use body cams for webcasting.
6. **Examine ballots:** for each ballot, display marks; record voter intent per contest.
7. **Capture snapshot:** capture an image or scan of each audited ballot and display on screen; associate with ballot ID; record linkage. Use simultaneous webcasting and video recording.
8. **Enter results:** input interpretations into the audit system in view; record entries. Simultaneously record votes as captured in any computer interface and also on paper records.
9. **Update risk:** run calculation; display updated p-value/risk metrics of all contests; record results.
10. **Iterate or stop:** if stopping condition not met, generate additional sample using same seed procedure; record each iteration.

### Recording (PTP Sheet)

Seed generation (all rolls), parameters, sample IDs, per-ballot interpretations, system outputs per round, decision point, sheet ID linking to any images.

### Public verification

Observers verify randomness generation, parameter entry, ballot retrieval, interpretation entries, and that system outputs correspond to entered data. Observers can independently recompute seed and confirm sample selection.

---

## 3. Ballot Collection and Chain-of-Custody PTP

### Purpose

Verify that ballots are securely collected, transported, stored, and logged without gaps.

### Inputs

Collection points (poll sites, drop boxes), transport logs, seal logs, storage logs.

### Procedure

1. **Collection event:** display empty container/seal; record seal ID; observers confirm. Verify that all envelopes, ballots, boxes are collected.

2. **Close collection:** at end of period, close container; apply seal; record time and seal ID.
3. **Transfer to transport:** record custody transfer (from/to, time, location); observers witness handoff. Possibly weigh the containers as they are collected and record the weight.
4. **Transport:** record departure/arrival times; no unlogged stops; observers may accompany or view via live feed.
5. **Intake at storage:** verify seal intact; record condition; log storage location.
6. **Periodic inventory:** perform counts or weight checks per protocol; record values; repeat if inconsistent; **record all attempts.**
7. **Access events:** any opening/resealing is performed in view; record reason, personnel, times, old/new seals.

### **Recording (PTP Sheets/Logs)**

Chain-of-custody log with timestamps, locations, personnel, seal IDs, condition checks, inventory values, sheet IDs and container weights.

### **Public verification**

Observers witness sealing/unsealing, custody transfers, and inventory checks; verify logs match observed events in real time.

---

## **4. Logic & Accuracy (L&A) Testing PTP**

### **Purpose**

Demonstrate that voting systems correctly record and tabulate predefined test ballots.

### **Inputs**

Test deck (ballots), expected results, system under test.

### **Procedure**

1. **Present test deck:** display ballots and **expected outcomes** before execution; record both.
2. **Initialize system:** show system state (zero tapes/config); record.
3. **Run test ballots:** feed ballots in view; observers can inspect each ballot before insertion.
4. **Produce results:** print or display results; record outputs.
5. **Compare:** compare results to expected outcomes; record differences.
6. **Repeat if needed:** rerun subsets if discrepancies occur; record each run.

### **Recording (PTP Sheet)**

Expected results, ballots run, system outputs, comparison results, discrepancies and reruns.

## Public verification

Observers verify expected results are known in advance, watch ballots being processed, and confirm recorded outputs match printed/displayed results.

---

# 4A. Logic & Accuracy (L&A) – Touchscreen BMD and End-to-End Tabulation PTP

## Purpose

Verify that ballot marking devices (BMDs) correctly capture voter selections on a touchscreen, produce an accurate voter-verifiable paper record (VVPAT/printed ballot), and that the resulting ballots are correctly scanned, transmitted, and aggregated by the tabulation system (EMS).

## Inputs

- Defined **test scripts** (selection patterns per contest, including edge cases)
- Expected results for each script (per ballot and aggregate)
- BMD(s), scanner(s), and EMS/tabulation system configured for the election
- PTP recording sheets (unique IDs) and optional capture devices (camera/scanner)

## Procedure

1. **Present test scripts and expected outcomes**

Display all BMD test scripts (e.g., straight ticket, split selections, undervotes, write-ins, overvote attempts where allowed) and the **expected results** (per ballot and aggregated totals). Record both on the PTP sheet.

*Public verification:* observers confirm scripts and expected totals are visible before testing begins.
2. **Initialize systems (BMD, scanner, EMS)**

Show zeroed state on BMDs and scanners; confirm EMS has no prior test data loaded (or that a clean test election is created). Record system identifiers (model, serial, software versions).

*Public verification:* observers confirm zero tapes/status and EMS setup.
3. **Execute BMD test scripts (in view)**

For each script:

  - a. An operator (or member of the public, if permitted) enters selections on the touchscreen exactly as specified.
  - b. Complete the ballot and **print the paper record**.
  - c. Display the printed ballot/VVPAT to observers.

*Public verification:* observers confirm the on-screen selections match the printed record.
4. **Record per-ballot results (real time)**

For each printed ballot: record the interpreted selections on the PTP sheet. If capture is

permitted, **photograph/scan** the printed ballot and link to the sheet ID.

*Public verification:* observers confirm that recorded selections match the printed ballot.

5. **Scan BMD-produced ballots**

Feed each printed ballot through the scanner in view. Capture any scanner messages or error conditions; record them.

*Public verification:* observers confirm each printed ballot is the one scanned.

6. **Scanner output verification (per ballot, if available)**

Where scanners provide per-ballot cast vote records (CVRs) or logs, display or export them and **link each CVR to the corresponding ballot ID**. Record key fields on the PTP sheet.

*Public verification:* observers confirm CVR entries match the printed ballot interpretations.

7. **Transmit/ingest to EMS (aggregation path)**

Demonstrate the **transfer of scanner results to the EMS** (e.g., removable media import or network transfer) in view. Record method, timestamps, and file identifiers.

*Public verification:* observers confirm the exact files/media used for transfer.

8. **Aggregate results in EMS**

Run tabulation/aggregation in the EMS and display totals by contest. Record the results.

*Public verification:* observers confirm totals are visible and recorded as displayed.

9. **Compare to expected outcomes**

Compare aggregated EMS totals to the pre-published expected results. Record matches/mismatches.

*Public verification:* observers can recompute totals from recorded per-ballot entries and confirm agreement.

10. **Discrepancy handling and repeats**

If any mismatch or anomaly occurs (BMD print mismatch, scanner misread, transfer error, EMS discrepancy):

- Isolate the step, repeat the affected portion, and **record each attempt**.
- Document resolution or remaining discrepancy.

*Public verification:* observers witness all repeats and confirm all intermediate results are preserved.

11. **Closeout**

Document final status (pass/fail by component and end-to-end), system identifiers, and seal/handling of test ballots. Archive PTP sheets and any linked images.

## **Recording (PTP Sheet)**

- Header: date/time, location, test election ID, device IDs (BMD, scanner, EMS)
- Test scripts and **expected results** (pre-listed)
- Per-ballot entries: selections, ballot ID, optional image reference
- Scanner events and per-ballot CVR linkage (if available)
- Transfer details (media/file IDs, timestamps)
- EMS aggregated totals
- Comparisons (per contest) and discrepancy logs (all attempts)

- Sheet ID (QR/data matrix) linking all artifacts

## Public Verification Points

- Scripts and expected results are disclosed **before execution**
- Touchscreen selections → printed ballot correspondence is visible
- Each printed ballot observed is the one scanned
- Any per-ballot CVR (if available) matches the printed ballot
- Transfer into EMS is observed (no hidden ingestion)
- EMS totals match both expected outcomes and independently tallied per-ballot entries
- **All intermediate attempts** (including any failures and retries) are recorded and visible

## Notes

- The protocol verifies **both the marking function (BMD)** and the **end-to-end tabulation path** (scan → transfer → EMS aggregation).
  - Where systems do not expose per-ballot CVRs, the protocol relies on the preserved linkage between **printed ballots and observed scanner ingestion**, plus aggregate reconciliation.
  - This procedure should be executed on representative BMD models and across all ballot styles used in the election.
- 

## 5. Hash Verification PTP (reference procedure)

### Purpose

Verify installed software matches certified versions via hash comparison. Note: Hash verification is important but does not mean the software or device cannot include malicious back doors or other vulnerabilities, as these may be included in the certified version.

Please note: certified hash values commonly excludes certain files, such as configuration files, which may be incorrect as well. Therefore, hash value comparison is not a substitute for full Logic and Accuracy testing and post-election auditing.

### Procedure (summary)

1. **Device to Be Verified:** The responsible officials present the recording sheet and identify the device to be verified, including model and serial number, in view of observers.
2. **Certified Hash Value:** The certified hash value is obtained from an independent, authoritative source (e.g., official publication or website) in view of observers. The full value is displayed and read aloud. [This may require a device connected to the internet]

3. **The certified hash value is recorded** in real time on the recording sheet in human-readable form. Observers verify that the recorded value matches the displayed value.
4. **Voting system hash value:** The voting system produces its own hash value through a documented process, and is probably printed out. The resulting value is displayed and read aloud in view of observers.
5. **The device-reported hash value is recorded** in real time on the same recording sheet in human-readable form. Observers verify that the recorded value matches the displayed value.
6. **Machine readable capture:** A fixed subset of leading characters (e.g., the first 6–8 hexadecimal digits) from each hash value is recorded in structured fields designed for comparison and machine-readable capture. Observers verify that the subset matches the corresponding portion of the full values.
7. **Full hash value is the official hash.** The structured subset fields are compared visually to determine whether they match. The full hash values are then compared to confirm consistency. The comparison result is recorded.
8. **Repeat as needed.** If any discrepancy or uncertainty arises, the process is repeated, and each result is recorded separately on the same sheet. All intermediate values and repeated measurements are preserved as part of the official record. If the hash values do not match, then the version of the code is incorrect.
9. **Reporting:** The completed recording sheet, including all values, intermediate results, and comparison outcomes, is made available for inspection and, where applicable, scanning or digital capture.

This procedure ensures that acquisition of values, recording of those values, and comparison of results are all observable and verifiable in real time. The use of structured fields allows both human verification during the process and reliable post-process analysis without transcription.

This example demonstrates how real-time verification, structured recording, and public observation can be combined in practice.

#### **Public verification**

Observers witness source retrieval, device output, recording, and comparison.

---

## **6. Real-Time Backup and Preservation PTP**

### **Purpose**

Ensure that critical election data (e.g., ballot images, cast vote records (CVRs), logs, and tabulation data) are captured, verified, and preserved at regular intervals throughout the election lifecycle, with public visibility into the process.

## Scope

Applies to all systems that generate audit-relevant data, including scanners, BMDs, and tabulation/EMS systems.

## Procedure

### 1. Define backup schedule

Establish and publicly post a schedule for periodic backups (e.g., hourly, per batch, or at defined processing milestones). Record schedule parameters. Typical events will be after Early Voting, Election day, Post Election day processing, and daily during mail ballot processing.

*Public verification:* observers can see and confirm the schedule in advance.

### 2. Identify data sources

Identify and display the data sources to be backed up (e.g., ballot image directories, CVR exports, logs, EMS databases). Record system identifiers and storage locations.

*Public verification:* observers confirm sources match declared systems.

### 3. Initiate backup event

At the scheduled time, initiate the backup process in view of observers. Record timestamp and operator.

*Public verification:* observers witness the start time and initiation action.

### 4. Capture data snapshot

Generate a snapshot of the relevant data (files or database export). Record file counts, sizes, and identifiers.

*Public verification:* observers confirm that snapshot reflects current system state.

### 5. Compute integrity values

Compute cryptographic hash values (e.g., SHA-256) for the backup dataset or manifest. Display and record values.

*Public verification:* observers verify that recorded hash values match displayed values.

### 6. Record structured summary

Enter key values on the PTP sheet, including:

- timestamp
- dataset identifier
- file count
- total size
- hash value (full + structured subset if used)

*Public verification:* observers verify real-time recording.

### 7. Secure storage of backup

Transfer backup to designated storage (e.g., external media, secure server, cloud)

repository). Record destination and transfer method.

*Public verification:* observers confirm transfer action and destination.

#### 8. **Optional public commitment**

Where policy permits, publish or commit hash values (e.g., public log or website) to create a time-stamped integrity reference.

*Public verification:* observers confirm values match recorded sheet.

#### 9. **Repeat at scheduled intervals**

Perform subsequent backups according to schedule. Each backup produces a separate PTP sheet.

*Public verification:* observers confirm consistency across events.

### Recording (PTP Sheet)

- Header: date/time, location, system identifiers
- Backup event ID
- Data source description
- File counts and sizes
- Hash values (full + optional structured subset)
- Storage destination
- Operator(s)
- Sheet ID (QR/data matrix) linking to backup set

### Public Verification Points

- Backup schedule is known in advance
- Snapshot generation is visible
- Hash values are computed and recorded in real time
- Recorded values match displayed values
- Transfer to storage is observed
- Repeated backups follow declared schedule
- Archived backups can be matched to recorded hash values

### Notes

- This protocol provides a time-sequenced chain of evidence, reducing reliance on post-election reconstruction.
- It complements other audits by preserving intermediate system states.
- When combined with Public Transparency Protocols for other processes, it enables continuous, verifiable auditability throughout the election lifecycle.

## 6. PTP Recording Sheet (applies to all procedures)

Each PTP produces one or more sheets containing:

- Header: date, location, procedure type, identifiers (batch/ballot/device), personnel
  - **Full values** (human-readable)
  - **Structured fields** for key values (fixed-position digits/marks for machine capture)
  - Intermediate results (all attempts)
  - Comparison outcomes and notes
  - Unique sheet ID (QR/data matrix) linking to any digital artifacts
- 

### Closing note

These procedures demonstrate how **observable actions, real-time recording, and immediate public verification** are combined. The same pattern can be applied to additional processes by preserving the invariants of the PTP Framework.

These procedures are no doubt incomplete and will need to be further refined with input from the public.