

## Citizens Oversight Projects

771 Jamacha Rd, #148

El Cajon, CA 92019

[raylutz@citizenoversight.org](mailto:raylutz@citizenoversight.org)

<https://AuditEngine.org>

voice: 619-820-5321



<<StaticTitleBlock>>

**Date:** <<TODAY>>

**REF:** [M2047](#)

### **Subject: Election Record Security and Backup Practices**

Greetings:

Recent federal actions, including the seizure of ballots and election data from Fulton County, GA, and Riverside County, CA, have highlighted how election records may become the subject of investigative seizure when discrepancies are alleged. This situation underscores the importance of ensuring that election jurisdictions maintain secure, independent copies of critical election records so that transparency, verification, and public confidence can be preserved even if physical records or systems are removed from local custody or lost, such as due to natural disaster.

#### **Secure Snapshot Backups**

We encourage you to ask election offices to secure backups of data exported from election systems when that data becomes available in the normal workflow. These may be snapshots of all ballot images up to that point or incremental data backups if they are available.

When available, export two copies of the ballot images scanned so far and store them in two separate secure off-site safes located in secure government buildings. Maintaining two identical backups in two separate secure locations provides resilience against both physical loss and investigative seizure. USB drives are relatively inexpensive, compared with the cost of losing precious ballot data.

#### **Suggested Procedures:**

##### **Scanning at Polling Places:**

When ballot scanners are closed, ballot image data and Cast Vote Record (CVR) data can be transferred to the Election Management System (EMS) and then snapshot backups can be created. Normally, this means there will be at least one backup after early voting is completed, and then one or more after data is returned and uploaded to the EMS after the close of polls on election day.

**Central Scanning:**

Snapshot backups can be created at the end of each day of scanning of mail ballots and provisional ballots when they are processed.

**Other Data:** Where possible, the election office should also back up CVRs, e-pollbooks, logs, and other digital records, including the final set of ballot images.

Where possible, election management systems should produce and publish SHA-256 hashes or digital signatures for each data export. Publishing hashes does not reveal the data itself.

**Disaster Recovery and Continuity**

Even if an Election Management System were removed from service, ballot images and related data could still be analyzed using the same brand of equipment in another jurisdiction, or third-party auditing platforms capable of tallying ballot images across vendor systems.

We respectfully encourage your office to consider piloting these practices for some existing records or for an upcoming primary or special election and, if successful, incorporating them into standard operating procedures for November.

Respectfully,



Ray Lutz  
Executive Director, Citizens Oversight

Submitted on behalf of Citizens Oversight and supporting contributors.

P.S.

Additional Information:

[https://auditengine.org/docs/user-guide/rapid\\_data\\_backup/](https://auditengine.org/docs/user-guide/rapid_data_backup/)

If you encounter any problems with backing up your data, please let us know so we can update these instructions. Thanks!