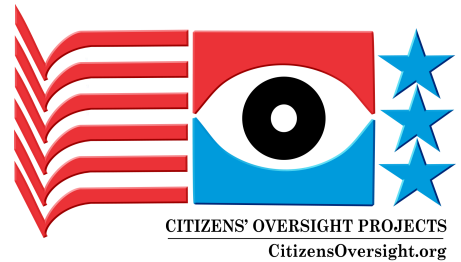


## Citizens Oversight Projects

771 Jamacha Rd, #148  
El Cajon, CA 92019  
[raylutz@citizenoversight.org](mailto:raylutz@citizenoversight.org)  
<https://AuditEngine.org>  
voice: 619-820-5321



**April 6, 2026**

**REF: [M2048](#)**

**TO: California State Senate Elections and Constitutional Amendments Committee**

**Re: Comments on SB 970 – Proposed Amendment to Elections Code §3101(c)**

To Members of the Committee:

The proposed addition to Section 3101(c) is too broadly framed to ensure a secure and auditable system for ballot return. The phrase “secure electronic transmission methods” does not establish enforceable technical boundaries.

**We do not support the current bill without the additional provisions described below.**

### **Baseline: Existing Mail-Based System**

The current system allows voters to mark a paper ballot by hand and return that ballot by mail for processing and audit. This provides a clear standard:

- the voter’s markings are the authoritative record
- the ballot can be directly inspected by humans
- votes are not encoded by QR codes or barcodes
- voter identity is validated using a signed return envelope
- voter privacy is preserved by separating identity from the voted ballot

Commonly, "fax" is used by election offices for ballot return. Modern fax systems frequently rely on multi-hop, store-and-forward transmission over internet infrastructure, with no or inconsistent end-to-end encryption and exposure of document content to intermediary systems. This approach must be banned.

### **Voter Validation and Privacy**

A complete system must address both voter authentication and ballot secrecy. Voter identity must be verified through a signed declaration comparable to the return envelope used in vote-by-mail. The voted ballot must be separated from identifying information prior to processing. Election officials must be able to validate eligibility without linking the voter to ballot selections. Procedures will need to be developed for handling printed ballots with coversheets in a manner that preserves voter privacy within the election office.

### **Controlled Devices**

The statute must not allow systems that rely on personal devices, as personal devices cannot ensure endpoint integrity. Instead, both end points of the secure communication must operate on controlled equipment in controlled environments. Transmission must originate from devices under the

administrative control of a governmental entity. Each device must be configured to prevent the installation or execution of unauthorized software. Each device must also be operated within a physically secured environment.

### **Location of Devices**

Sending devices should be located in controlled environments such as military bases and United States diplomatic facilities, where voter identity can be verified and use of the system can be supervised.

The SOS should consider receiving at a centralized state-operated facility or selected county office, rather than at all individual county offices. Centralized receipt reduces operational overhead, limits the number of exposed endpoints, and reduces the overall attack surface. Ballots can then be distributed in bulk to the appropriate county election offices for standard processing and audit.

### **Preservation of Voter Intent**

The voter's marked ballot must remain the authoritative record, and systems that interpret or reconstruct selections introduce risk. The ballot must be transmitted as a faithful image of the voter-marked paper ballot. The printed ballot must be a direct rendering of the transmitted image. The system must have no knowledge of ballot content beyond reproducing the image.

### **Certified Devices and Direct Transmission**

Both sending and receiving devices should be reviewed and certified to ensure that they faithfully transmit and reproduce ballot images without alteration.

- Transmission should occur directly between originating and receiving devices
- The system must use end-to-end encryption with mutual authentication
- No intermediary systems may store or process ballot content
- A coversheet may be used to specify the receiving elections office in a machine-readable format
- The system must validate that destination against trusted configuration prior to transmission
- The system must verify integrity and provide confirmation of receipt and processing.

### **Proposed Language**

(c)(1) The Secretary of State shall promulgate regulations to facilitate the secure return of ballots from military or overseas voters through secure electronic transmission methods that comply with the requirements of this subdivision.

(2) Any such method shall be limited to the transmission of a voter-marked paper ballot as a non-reinterpreted image and shall not permit ballot marking or vote selection on a personal electronic device. QRcodes or barcodes that encode votes shall not be used.

(3) Ballot transmission shall originate only from devices under the administrative control of a governmental entity, including military installations or United States diplomatic facilities, that are configured to prevent the installation or execution of unauthorized software and are physically secured.

(4) Both the originating and receiving devices shall be reviewed and certified by the Secretary of State to ensure they faithfully transmit and reproduce ballot images without alteration. Availability of these devices must be carefully restricted and the receiver only

accepts transmissions from known certified devices. These transmitting devices must not be personal electronic devices.

(5) The transmission shall occur directly between the originating device and the receiving election official using end-to-end encryption and mutual authentication. No intermediary system may store or process the content of the ballot in unencrypted form.

(6) The receiving system shall produce a paper ballot that is a faithful and complete rendering of the transmitted image and shall not interpret or reconstruct voter selections, and shall operate without semantic interpretation of ballot content. A single county may be selected for receiving all ballots for California, and it would then send to the other counties using conventional courier.

(7) The system shall include mechanisms to verify the integrity of the transmitted ballot and to provide confirmation of receipt and processing to the originating device.

(8) A machine-readable coversheet may be used to specify the intended receiving elections office, and the system must validate that destination against trusted configuration prior to transmission.

(9) A second coversheet should be an affidavit executed by the voter, including the voter's signature and identifying information comparable to that used in vote-by-mail systems and to ensure separation of voter identity from the voted ballot prior to tabulation. Additionally, the government office could witness the voter's identification and sign the affidavit accordingly.

(10) The Secretary of State shall adopt additional regulations to ensure that ballots returned under this subdivision are auditable using procedures equivalent to those applied to other paper ballots.

## **Conclusion**

The goal of enabling ballot return for military and overseas voters is important, since overseas civilian mail is not always secure. Any electronic method must meet the standard established by the existing mail-based system, including voter validation and privacy protections. Clear constraints on device control, transmission integrity, and faithful reproduction are necessary to preserve ballot integrity and public confidence.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'Ray Lutz', with a stylized flourish at the end.

Ray Lutz, Executive Director, Citizens Oversight