**Citizens' Oversight Projects (COPs)**
771 Jamacha Rd #148
El Cajon, CA 92019
CitizensOversight.org
619-820-5321

June 22, 2020

This document available here: https://copswiki.org/Common/M1946

# COMMENT ON VVSG 2.0

Dear Chair Hovland and Director Harrington:

We respectfully submit the attached comments on the next iteration of the Voluntary Voting System Guidelines (VVSG 2.0) for review and consideration.

Although our representative, Ray Lutz, and other endorsers have or may have also participated in the extensive submission by the State Audit Working Group (SAWG), the following items are highlighted in this separate submission.

This document deals with the following subjects:

1. The overall scope of the VVSG should include central count voting system functions applicable to vote-by-mail voting.
2. Support of Ballot image audits.
3. Support of remote attestation and software validation.
4. Guidelines and terminology to promote voter-verification
5. Support of Audit Oversight by the Public

Items 2 and 3 include provisions to improve the security and trustworthiness of voting machines and allow for independent automated audit techniques.

# 1 Overall Scope should include Vote-by-mail and absentee voting and central count

### 1.1 Justification

Many states are now using Vote-by-mail (VBM, also sometimes called "absentee" or "at-home") voting as the primary means of voting. Some states, (CO, OR, WA) are now "all" VBM states, with VBM ballots being sent to all registered voters, although in-person voting is still provided at central offices and sometimes in vote centers. Western states, such as CA, have recently found that more than two-thirds of voters choose to vote by mail. VBM is popular among voters because the experience is more like a take-home test rather than a pop-quiz.

This year, we are also faced with a critical need to provide safe voting during the COVID-19 global pandemic. As a result, more states are embracing VBM voting as a safer alternative to in-person voting at precinct polling places or voting centers, where it is difficult to maintain social distance and voters will come into contact with common equipment and surfaces.

Especially because this topic has become politically charged, the VVSG should encompass VBM and similar voting methods.

The document does deal to some extent with hand-marked paper ballots, such as the font size, size of the target "bubble" to be marked by the voter, and the like. Many districts use voter-facing scanners that accept hand-marked paper ballots. In the case of VBM voting, central count scanners are typically used. This central count scenario is largely only touched upon by the requirements in the VVSG, such as isolation from public networks, provisions to enable audits, and the like. For example, in Colorado, they use central count scanners which provide optional imprinting of unique identifiers on each ballot such that the cast-vote record can be paired up with the physical ballot to support ballot-comparison statistical audits. (These identifiers do not link the ballot back to the voter because they are applied after the voted ballots are permanently separated from the identities of their voters.)

### 1.2 Recommended specific changes.

There are procedures and paper-based systems that SHOULD be included in the requirements, in our

view, regarding the following:

1. Guidelines for VBM envelope design and procedures, such as mandatory bilingual (not non-English monolingual) envelopes and ballots to mitigate VBM's additional opportunities for unconscious and conscious bias by temporary workers and officials approving envelope postmarks and signatures, as well as whole ballots and individual ballot lines.
2. Guidelines and procedures regarding VBM voters who may choose to vote in the precinct or vote center, such as when using a provisional ballot, to ensure that multiple ballots cannot be cast in the name of a single voter.
3. Guidelines and procedures for systems that scan and validate signatures.
4. Guidelines and procedures for curing missing or mismatched signatures.
    - One issue: Require that election jurisdiction personnel conducting VBM signature verification have false positive and false negative scores. Purpose is to document the viability of the signature verification process. Personnel with high score(s) to be removed from position.
5. Guidelines and procedures regarding special reports that are appropriate for use of VBM voting.
6. Guidelines for central-count scanning that may differ from machines that operate in the local situation.
7. Procedures to allow for oversight of the above given COVID-19 concerns.

Our organization will be happy to participate in a consensus-based process to more fully define these provisions.

## 2. Support of ballot image audits

### 2.1 Justification

Modern election equipment from all vendors that process hand-marked paper ballots or ballots marked by a ballot marking device (BMD) utilize scanners that capture "ballot images." Ballot images are relatively high resolution bit-map images of the ballot, one for each side. Sometimes, these products utilize commercial-off-the-shelf (COTS) scanner devices which are not specifically designed for use in elections, or the scanner may be integrated into equipment specifically designed for voting. In either case, these devices all operate the same way. They first produce document images, and then capture votes from the

images by application of image processing software to recognize and interpret marks on the ballot as voter intent.

The ballot images thus have a 1:1 correspondence with each ballot, and what can be seen may be nearly indistinguishable from the original paper ballot. The created ballot images must be stored in memory or on disk prior to evaluation to determine voter intent. These recorded data, in whatever format, are thus public records, and must be preserved as election materials.

### 2.2 Recommended Changes

#### 2.2.1 Modify VVSG Text and Glossary regarding the term "Ballot Image"

The term "Ballot Image" now must be confined to mean a digital picture of the ballot, typically encoded into files such as PDF, TIF, PNG, or other formats. The glossary and text throughout the VVSG must change to actively deprecate prior meanings of the term. In the past, this term was used to mean:

- The summary of the vote as provided by a DRE machine after the user has completed voting.
- The cast-vote record, either in tabular form or as a separate report summarizing the votes as determined by the election system after reading the ballot.

We believe that the definition of the term "ballot image" should mention these other prior uses that are now deprecated.

#### 2.2.2 Securing Ballot Images

Any and all ballot images from a scanner of hand-marked paper ballots or BMD ballots must be frozen for later authentication. This act of securing the ballot images must occur as soon as possible after scanning using cryptographic signatures to allow for detection of any subsequent changes of those images, and to enable ballot image audits. The goal of these changes is to make it infeasible to undetectably modify ballot images once they are secured.

The proposed process is to produce a secure hash digest of each raw image, that is, just the bits without any, or with only minimal formatting or encoding, and no compression. Even if the image is later placed in another format (such as PDF, TIF, or PNG), it must be feasible to extract just the raw image, recalculate the secure hash, and then compare the hash provided by the device, which is also signed by that device's secret key. Digests and images must be sent together when polls are closed. Note that to support this

method, lossy compression methods, which are available in formats such as JPEG or JBIG must not be used. Encryption of data for transport is not restricted as long as the resulting images are decrypted and can be later independently compared. We propose this change to the VVSG text:

> **9.2-H Cryptographic security of ballot images**
>
> Ballot images should be secured as soon as possible, preferably using a private key maintained in a Hardware Security Module, and including a signed cryptographic hash of the uncompressed and unformatted bit image. The method used must allow comparison with the image after it is converted to other formats, such as PDF, PNG, TIF, etc. which includes internal non-lossy compression, but which will then allow the uncompressed image to be compared with the signed cryptographic hash.

### 2.2.3 Using OCR-compatible paper ballot format

To support ballot image audits it is essential that the simplistic precinct-based election scanners accurately image the ballots. Changing the ballot format slightly to support such audits can go a long way to improving the performance and reliability of a ballot-image audit that uses the ballot images actually produced by the voting system.

**Recommended changes:**

> **9.2-I OCR-compatible paper ballot format**
>
> To the extent practicable, hand-marked and BMD ballot formats must be compatible with Optical Character Recognition (OCR) processing, as follows:

- Use all white background with black lettering and avoid the use of gray-scale background.

- Each ballot line header, or title, must identify its contest without having to refer to the ballot style. For example, use "Mayor City of Butte" not just "Mayor" on the Butte ballot. Utilize the same title names in the cast vote record and on BMD summary printouts. Adding to the ballot line title a contest-identifying numeric value or tiny QR code facilitates efficient audits by eliminating extensive manual alignment of the contest with the ballot style.

- Avoid deliberate the use of "drop out" of colors (e.g. red) that are not visible in the image.

- Provide alignment blocks in all four corners of the ballot and regular timing marks to allow

registration of the image and correction for uneven scanning speeds. Alignment blocks should provide easy recognition of the orientation and side of the ballot.

- Encode the ballot sheet style on the ballot using bar or QR code. Ballot sheet style should have a 1:1 correspondence to the contests, party, sheet number, and language of the ballot sheet. If multiple precincts use the same style, the precinct number should be separately indicated and encoded. This is to allow a single style analysis to be used for multiple precincts when the only difference is the precinct.

- To preserve anonymity (ballot secrecy) the number of sheet styles should be minimized. To preserve voter anonymity, styles should not be needlessly subdivided.

- The style designator should map directly to a single ballot style, in terms of which contests are included, and the layout and format of the ballot, including language, option order, sheet, and party. The mapping should be unique and singular, such that any other ballot sheet that has the same layout should use the same style designator.

- Draw lines around each contest and preferably also around each contest option to allow for automatic segmentation. These lines should be complete and visible in the ballot image, and not so thin that they are not included in the image.

- Ballot images should be imaged with at least 200 dpi resolution.

Furthermore, we believe a standard hand-marked paper ballot format should be defined such that all election equipment will use the same format and all voters will have the same experience.

## 3. Support "Remote Attestation" and software validation

"Remote Attestation" is now becoming a standard feature in "Internet of Things (IoT)" devices. It is a common problem: When a device is contacted, is it really the expected device, or is it an impostor? In the world of voting systems, voter-facing equipment in polling places are not connected to the internet. So the usual multiple-round "handshake" protocol that is common and standardized when communicating with IoT endpoints is not available in its entirety. But a single request and response transaction is possible since the equipment is configured with first with a USB Drive (or other portable memory device) with information from the Election Management System (EMS), and then and the end of the election day, the

USB Drive is returned to the EMS with the response, as well as the cast vote records and ballot images.

### 3.1 Single-round attestation

We propose that the single-round handshake include a request for the attestation record. At the end of the voting session, the equipment can write the attestation record to the USB Drive, and then when the USB Drive is returned to the central office, this attestation record can be validated and published for public review.

At a minimum, the voting equipment should provide a signature based on the private key secluded in a Hardware Privacy Module which is infeasible to access, and which can be evaluated using the public key of the device which is known and published by the EMS. The initial configuration data should include a random "nonce" to make sure the device cannot just return a constant value that could be easily faked. Although we have proposed a single-round protocol in the companion document referenced below, the remote attestation protocol may be better modeled after the industry standard approach as used in IoT applications.

### 3.2 Software/Firmware validation

We also propose that the attestation record include a secure hash digest of the complete embedded firmware. This secure hash digest can be checked against an active escrow service that not only maintains a copy of the officially certified firmware, but allows anyone to check that the hash digest provided in the attestation record is produced by the escrowed code when provided the same nonce. A similar procedure can be used to also validate the software used in the EMS system and any non-COTS scanners.

The details of these two proposals is provided in this document:
"**Securing Digital Ballot Images to Enable Auditing**" -- https://copswiki.org/Common/M1936

## 4. Guidelines and Terminology on the Ease of Voter-verification

Throughout the VVSG draft, the terms "Voter Verified" and "Voter Verifiable" are used. Different types of voting have different levels of "ease" of voter verification. We propose that these terms be defined and the requirements are that ballots are *fully* and *directly* voter verifiable. These criteria should also be applied and treated as requirements with the newly suggested "Remote BMD" systems, where a user votes at home and prints out a paper ballot which can be submitted either by mail or by hand delivery.

### 4.1 *Fully* Voter Verifiable vs. *Partially* Verifiable

The term "voter verifiable" should be enhanced to clarify this distinct difference:

**"*Fully* Voter Verifiable"** -- The voter can see on the paper ballot record both the options they selected and all the options they did not.

**"*Partially* Voter Verifiable"** -- The voter can only see the selections they made.

VVPAT devices and many BMDs provide *partial* voter verifiability. Ballot summaries on ES&S Express Vote and Los Angeles's VSAP (voter system for all people) systems are only partially voter verifiable because they include only the options the voter selected.
The full paper ballots, as used by Dominion, Hart, and Clear Ballot, and that provide a full bubble-type hand-markable paper ballot can be marked (or created by) a BMD device. Those are "*fully* voter verifiable".

It is critical that we enhance this term to distinguish this difference.

**Why is this important?**
By inspecting the ballot after the election, it is not possible to know what occurred during the private touch-screen session with the voter. The only evidence is what is printed or marked on the ballot, and that limits what the voter can verify.

BMD devices that utilize a touchscreen have a limit on the number of ballot options that can be shown at a time. For example, the VSAP system used in LA can only display four candidates per screen. That system provides a "MORE" button at the bottom but a voter does not have to look through all the options before moving to the next contest using the "NEXT" button. So those candidates at the top may have a substantial advantage, and the voter may not even realize that more options are indeed available.[1]

The design of this system does not force the user to scroll through all the pages of options with MORE before moving to the NEXT contest.

The printed ballot in this case is a selections-only type which only lists the options the voter voted for, and does not list the options the voter did not vote for but had the option to do so (or should have). Thus, it is not possible to fully verify their vote, just by looking at this printout. Were there more candidates? Was the voter shown all options? There is no way to tell by reviewing this official record. If, for example, the

[1] See https://laist.com/2020/01/23/beverly-hills-files-lawsuit-sues-la-county-over-ballot-design-skip-candidates.php

voter did not understand that there were indeed more than the four candidates shown in the case of the VSAP example, then by looking at the printed ballot that lists all the other options not selected, that voter could then discover that there were more options, and then ask to revote if they see the option they wanted to vote for but did not see it on the screen. So *the printed record* should allow the voter to conduct a full review of the options selected and those that were not selected.

A partially verifiable printed record is in contrast with the conventional hand-marked paper ballot with targets that are marked to indicate the selection. By definition, the voter can see the options they voted for and the options they did not vote for. It is thus "fully verifiable."

### 4.2 "Simultaneous" and "Witnessed" criteria

Also, there has been talk about "Voter Marked" vs. "Hand Marked" ballots. Is a BMD marking a ballot equivalent to someone marking the ballot with their own hand holding a primitive marking device (like a pen)? Not exactly, to be sure. With existing typical BMD designs, the voter can't watch the mark being made, while with the hand-marked paper ballot, your own hand is making it, and you can watch the mark being made on the ballot. The difference has to do with how closely correlated the action of the voter is to the marking of the ballot. Some BMD devices, like most of those that are ADA compliant, have a first operation where the voter makes selections electronically, a second operation where the ballot is marked, and a third operation where the voter can review the ballot. The action of the voter is not simultaneous with marking, and the marking is not witnessed by the voter, as it is done inside a printer device[2]. True hand-marking is **simultaneous** with the action of the voter, and the marking is **witnessed.**

If a BMD device had a second verification phase, it could assist the voter in checking that the printed record matches the on-screen selections. BMD devices should include this "active verification" phase.

### 4.3 *Direct* vs. *Indirect* Verifiability vs. *Unverifiability*

Another aspect of voter verifiability has to do with whether the voter can **directly** verify, without any additional assistance, what the computer will eventually interpret as their voter intent.

With hand-marked paper ballots where the user marks targets, the voter can easily and directly see the

---

[2] Although current BMD devices use laser or thermal printers where it is not possible to watch the marks being made, technology may be feasible that automatically mark the ballot AND allow the voter to watch the marks being made, and thus it is not simultaneous but it is witnessed. For example, an ink jet printer where the user can watch the marks being printed might be such a device.

marking that they made on the ballot and therefore verify what the computer will interpret. There is no further conversion required. (We must note here that the design of the ballot should be clear which targets are associated with which options. Sometimes right-justified targets for left-justified options will place the target closer to the next column and confuse the voter. Correcting this problem should be part of the VVSG guidelines).

With BMD-marked paper ballots that have the same format as a hand-marked ballot, and which do not use barcodes or QR codes to encode the vote, the voter can also directly verify their vote without any assistance, and thus they are *directly* (and *fully*) verifiable.

For BMD ballots that use barcodes or QR codes, *direct* verification is not possible. But with the use of a smartphone, for example, it may be possible to read the barcodes or QR codes and determine what is encoded. This is a common function in most modern smartphones or it can be added as an app. Then the question will be whether the user can easily interpret the decoded data to confirm that what they voted for is indeed what is encoded in the machine readable code. Then it is ***indirectly* verifiable**, but certainly this is not as available nor as easy as the directly verifiable case.

In the case of the Los Angeles VSAP system, the QR codes encode the vote using alphanumeric characters, like K9, or T5, which indicate that the voter voted for a particular option. Those values are printed on the ballot next to the human-readable text. The codes for a given option are also consistent among all ballot styles, so a simple look-up table can confirm that across all ballots, T5 means a specific option.

Unfortunately, with the ES&S ExpressVote BMD and the Dominion ImageCast BMD, it is not at all easy to interpret the values from the barcodes or QR codes. There is no direct and consistent relationship between the code and what is on the ballot, and there is nothing printed on the ballot to match up. The ExpressVote does not use consistent values across ballot styles, while the ImageCast uses a binary format that can only be decoded with extensive additional information. Because neither of these BMDs exhibit either direct or (easy) indirect verifiability, they are **unverifiable**.

Fully electronic voting systems have been proposed that encrypt the voter's selections early-on, and then use homomorphic encryption[3] to keep the voter's selections encrypted even while they are included in the tabulation (or other methods that may not encrypt the ballots). These have been called E2E-V systems.

[3] https://en.wikipedia.org/wiki/Homomorphic_encryption

The question will be whether the voter can fully and directly verify the voter's selections without any additional assistance, and thus confirm that their votes are included in the encrypted record. To date, E2E-V solutions provide neither full nor direct verifiability.

### 4.4 The ideal voting system

The ideal voting system will have all the following properties:

Fully and directly voter verifiable -- Voter can verify options chosen and those not chosen

Simultaneous marking with voter action -- verification can be done when voter takes action

Witnessed -- Voter witnesses marking of the ballot as the mark is being made.

**BEST** The only voting system that provides all properties at this time is a conventional **hand-marked paper ballot**. Such paper ballots can be pre-printed or printed on demand.

**GOOD** A close second is a BMD that creates a ballot in the **same format as a hand-marked paper ballot**. It does not provide simultaneous marking with voter action nor direct witnessing, because the marks are added to the ballot inside the printer, but the result is fully and directly verifiable.

**POOR** A BMD that uses QR codes or barcodes that can be matched up to the printed selections and verified using a published list. This is not *fully* nor *directly* verifiable, but it is *partially indirectly* verifiable. The Los Angeles VSAP system works this way, as it provides a list of selections with consistent alphanumeric codes that are used in the QR code, and can be checked in a published list. It is only *partially* verifiable because the entire list (include options that were not selected), and it is *indirectly* verifiable if the voter converts the QR code using any QR code app, and then reads the alphanumeric values and compares with the ballot, and with a published list. A published list is required because otherwise, the alphanumeric codes could be swapped and may not actually mean what the ballot claims that they mean.

**BAD** The bad solutions are BMDs that use QR codes or barcodes that are essentially impossible to verify without extensive additional information, and probably including E2E-V systems that require a separate application that may be able to solve cybersecurity algorithms, yet remain far beyond the understanding of the average person. E2E systems are still not demonstrated so we actually don't know how bad they really are.

On-demand ballot printing can print any of the many ballot styles, and the ballot can be checked when it is fed into the scanner for overvotes, as they are today. The BMD devices that do not have all these qualities should be only used for voters needing ADA assistance, and **non-verifiable non-verifying BMD devices should be banned.** As mentioned, BMD devices should include an "active verification" phase where the voter is assisted in checking the printed ballot.

## 5. Support of Audit Oversight by the Public

### 5.1 Justification

Audits of elections are now recognized as a key requirement to support election integrity. But election audits are generally performed by the same election officials and workers that were responsible for the canvass itself. Long ago, auditing professionals in other fields (such as finance) have recognized that the auditing team should not be the same people as those who are audited, because it is a simple matter to correct the audit results so that no discrepancies exist, implying that the election itself is clean as well. Although it seems like this would require malfeasance to occur, in the cases we have witnessed it appears it is more likely "innocent fix-up" of the audit rather than any true intent of fraud. Nevertheless, the result is the same, defeating the effectiveness of the audit by turning it into nothing more than theater. Therefore, audit procedures must provide adequate and standardized reporting sufficient for the public to review these results and verify the self-audits.

### 5.2 Canvass Result Reports to be Audited

The most important factor for thorough and efficient audit oversight is the existence of complete reports of results that are to be audited. The election equipment must therefore be able to provide these reports. Lack of such complete reports is the single biggest roadblock we have experienced in our attempts to provide audit oversight. Therefore, we offer this list of criteria we believe will result in our ability to provide thorough oversight of election audits:

- The tabulated results must be reported and frozen prior to any random selection process.
- A number of audit phases may exist, where a separate report is produced for that phase. It is common that there may be two phases: an election-night report, and then a later report that includes the later-arriving VBM ballots. The audit may further break down the results into groups, such as Early Voting, Election Day, Provisional, and Vote-by-Mail.

- The tabulated results must be broken down by the smallest unit of comparison. If a ballot-comparison audit is performed, the tabulated results must be broken down to the ballot. If a batch-comparison audit is performed, then the tabulated results must be broken down to the batch, and the ballots must be stored by batch, so that no additional handling is required. If a statistical polling audit is performed, then the final vote totals must be available for that phase.
- The report must include all auditable units in that phase, including those that are not eventually chosen for manual tally or other auditing methods. The sum of all auditable units in the phase must equal the official reported totals for that phase, and the sum of all phases audited must equal the final official results. Therefore, all ballots must be included in the audit universe, even though a subset of ballots is chosen for random review in many audit protocols.

### 5.2.1 Changes to VVSG

There are several places where the above requirements could be included. One is this section, where we have highlighted the recommended new text.

1.1.10 – Reporting Results

1.1.10-A – Post-election reports

The voting system must have the capability to create precinct post-election reports. If ballots are processed in a central-count operation by batch, or if ballots are processed at the polling place in vote-center operations that don't sort the ballots to the precinct, the election system must have capability to create a report of the totals of the votes in the contests included in each batch, such that it can be prepared prior to any random draw of a batch-comparison audit.

## 5.3 Use of Standardized Tally Sheets and Audit Reports

To enable audit oversight, it is critical that election audits are consistently reported. We have proposed two standards regarding reporting. The use of Uniform Tally Sheets and Uniform Audit Reports. Both sets of records are critical if statistical audits are performed. The following draft standards have been proposed:

- Uniform Audit Report:
    - https://copswiki.org/Common/M1940
- Uniform Audit Tally Sheets:

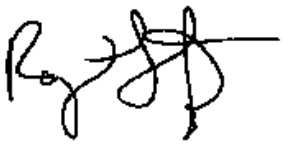
- https://copswiki.org/Common/M1939

These two documents will be attached to this comment in PDF form and are incorporated into this comment in full. We would be interested in participating in a consensus-based process to further refine these standards. We believe that although these are not part of electronic equipment, they are essential voting systems and procedures, and should be included per our opinion stated in Section 1.

## CONCLUSION

We hope that this comment to the VVSG 2.0 will be treated with seriousness and incorporated if at all possible, while still working to approve the guidelines as soon as is practicable. We notice a vast number of corrections and changes have been suggested and therefore recommend a second round of review.

Respectfully submitted,



Raymond Lutz
Executive Director
Citizens' Oversight Projects

Also endorsed by:

Harvie Branscomb
Election Process Improvement Advocate; harvie @ http://electionquality.com

Tim White
Washington State Resident and Election Integrity Activist

John Brakey
AUDIT-USA

REFERENCES

https://copswiki.org/Common/M1936 -- Securing Digital Ballot Images to Enable Auditing

https://copswiki.org/Common/M1939 -- Uniform Audit Tally Sheets

https://copswiki.org/Common/M1940 -- Uniform Audit Report