United States Election Assistance Commission
2023 Summary of Proposed Changes to VVSG

U.S. ELECTION ASSISTANCE COMMISSION
633 3rd St. NW, Suite 200
Washington, DC 20001

Introduction

In late 2002, Congress passed the Help America Vote Act of 2002 (HAVA), which created the U.S. Election Assistance Commission (EAC) and vested it with the responsibility of adopting Voluntary Voting System Guidelines (VVSG). These guidelines are used in the EAC's voting system testing and certification program (the program).

On April 5th, 2022, EAC Commissioners unanimously voted to adopt the VVSG Lifecycle Policy. The most recent version of this policy was adopted on June 16th, 2023. One aspect of this policy is to establish a consistent annual periodic review of the VVSG. The policy states that the EAC Testing and Certification Program Director will provide recommendations for updates to the VVSG that have been collected through the year from stakeholders in a report to the EAC Executive Director at the end of each fiscal year. The report will be shared with the Technical Guidelines Development Committee (TGDC), the Standards Board, and the Board of Advisors for consideration. Feedback from this process will inform the decision to make updates to the VVSG.

This report covers proposed VVSG changes that have been collected from stakeholders from October 2021 through June 2023.

Attachments

1. 2023 Spreadsheet of Proposed VVSG Changes

Summary of Proposed Changes to VVSG - 2023

As of June 30th, 2023, there have been a total of 250 proposed changes. These changes are shown in attachment 1. Sixty of these comments were originally submitted to the EAC in 2022 but have not previously been reviewed.

These 250 proposed changes have been reviewed by the EAC Testing and Certification team, who are responsible for maintaining the VVSG. The proposed changes have also been reviewed by the National Institute of Standards and Technology (NIST). As of the submission of this report, the VVSG subcommittee of the Standards Board and the VVSG Subcommittee of the Board of Advisors are also currently reviewing the changes. The EAC is looking forward to receiving their feedback and will review it when received.

The review of the proposed changes by both EAC and NIST indicate that:

- EAC and NIST largely agreed on responses to the proposed changes. 176 of the 250 of the NIST responses stated that they agreed with EAC with little additional comments.
- 47 of these proposed changes have broadly been accepted by the EAC. For the purpose of this report, acceptance means that these changes have been accepted in principle and it is felt that their inclusion in a future iteration of VVSG would enhance the VVSG program as a whole. The exact wording of these accepted proposed changes will need to be determined prior to inclusion in the next VVSG iteration.
- 17 items were not considered proposed changes but were comments that were noted. These will not require any further action by EAC. Most of these entries re-enforced requirements already in place in VVSG 2.0.
- 57 require further investigation and evaluation after review by EAC. This means that additional research is required to make a decision as to whether to accept or reject that change. This research may need to be done by EAC, NIST or another party. NIST are of the opinion that 28 of these should be rejected, and 9 should be accepted. The remainder still require further investigation.
- EAC and NIST disagree on 8 of the proposed changes. These are not fundamental disagreements on the requirements but include cases where it is felt that a change is already covered in another requirement.
- All other proposed changes were rejected as unsuitable for a new VVSG iteration.

It should be noted that, at the writing of this report, these proposed changes are still under review and are still being evaluated by the VVSG subcommittee of the Standards Board and the VVSG Subcommittee of the Board of Advisors. These boards may agree or disagree with EAC and NIST, and there may be further deliberation if there are disagreements. Therefore, the numbers shown above are subject to change.

Notable subjects of proposed changes

In the past there have been certain subjects within the VVSG that have generated more interest and commentary than others. For these proposed changes there are no subjects that significantly stand out from others, but some recurring thoughts include:

- Wireless

  There has been significant comment concerning the use of wireless communication and its prohibition. Much of this debate has centered on the method of enforcing prohibition. There remains some concern that the current requirements do not go far enough when it comes to prohibition.

- Barcodes

The use of ballots with barcodes is not new, and VVSG 2.0 and relevant test assertions cover this in some detail. However, there have been thoughts that it should be possible to decode barcodes with Commercial of the Shelf (COTS) equipment.

- Ballot Images and CVR (Cast Vote Records)

There are opinions that it should be a requirement that images of all sides of a ballot should automatically be saved when being scanned and cast. While systems do have the capability to capture ballot images, there are no requirements in VVSG 2.0 stating all images must be saved.

- End to End (E2E) Systems.

There are currently no verifiable E2E systems available on the market. It has been suggested that there be some change to E2E requirements.

- Remote Ballot Delivery, Marking and Return

There have been proposed changes to allow for remote digital ballot delivery, marking and return. This has traditionally been considered to be outside the scope of VVSG.

Conclusion

The intent of this effort is not necessarily to initiate a new VVSG draft in the short term. It is a collection of proposed or suggested changes to the most recent VVSG, in this case version 2.0, to consider each change in collaboration with the EAC's Federal Advisory Committees. Any proposed change may be accepted or rejected based on this consideration.

Following full consideration, those accepted changes may or may not initiate a new VVSG draft, at the discretion of the EAC and under advisement from its Federal Advisory Committees. Accepted changes that do not prompt initiation of a new VVSG draft will be carried into the next annual report of proposed changes to the VVSG. Rejected changes will be removed from the next annual report of proposed changes to the VVSG.

At the writing of this report, all proposed changes are still under review by the federal advisory committees. While there are proposed changes that have been provisionally accepted by EAC and NIST, these decisions are not final and may change.

It is highly unlikely that there will be any voting systems certified to VVSG 2.0 prior to the third quarter of 2024. While a voting system has been submitted, a test plan approved and test cases under development, there is considerable work ahead prior to certification.

Until there have been voting systems that have undergone the full testing and certification program to VVSG 2.0, any new iteration of VVSG will not capture 'lessons learned' of VVSG 2.0

in full. For this reason, it is recommended that no new iteration of VVSG be developed until one or more voting systems are certified to VVSG 2.0. The policy of reviewing proposed changes annually will continue and further approved changes will be maintained until formal development of the next iteration.

Attachment 1 - 2023 Proposed VVSG Changes

Date	Organization	VVSG	Requirement	Proposed Changes / Additions *Note that red indicates an addition to an existing requirement, and strikethrough indicates removal from an existing requirement.*	Comment / Reasoning	EAC Initial Decision	EAC comment	NIST Initial Decision	NIST Comment
6/21/23	Smartmatic	2.0	General	New CDF standards are being published by NIST. Is there a policy around their inclusion in VVSG?	Recommend establishing an effectivity policy for new CDF's.	Accepted	Only CDFs in the VVSG are required. New CDF publications will need to be added to a future VVSG revision in order to be required.	Agree with EAC decision	
6/7/23	Kevin Skoglund	2.0	General	The VVSG should monitor and encourage the use of memory safe languages.		Further Investigation	Further investigation to be done, reach out to NIST	No change needed	While memory-safe language usage is encouraged, it alone is not sufficient to ensure memory-safety. Thus, language usage is but one best-practice, but other factors are involved as well.
6/7/23	Kevin Skoglund	2.0	General	The VVSG 3.0 should require full-disk encryption on all hard drives.		Further investigation	Seems a good idea on workstations / servers. Less so on voter facing devices. Potential pitfalls should not been overlooked.	No change needed	Full disk encryption is not needed because cryptographic integrity protection is already required and confidentially is not needed during this phase of voting.
6/7/23	Kevin Skoglund	2.0	General	The VVSG 3.0 should prohibit voting systems from tabulating using ballot selections stored in barcodes.	Barcodes introduce a new attack surface and add risks to the voting system. Barcodes are legally problematic when they are used to encode ballot selections. HAVA requires each state to define what constitutes a vote for each category of voting system. If ballot selections appear on a ballot twice, once in a barcode and once as human readable text, then which representation holds the official votes? If the official votes are the barcode, then the voting system does not "permit the voter to verify (in a private and independent manner) the votes selected by the voter on the ballot before the ballot is cast and counted" as required by HAVA	Further Investigation required	Jurisdiction determines what is the "official vote"	No change needed re barcodes. Agree re official vote.	Nothing significant has changed about barcodes since VVSG 2.0
6/7/23	Kevin Skoglund	2.0	General	The VVSG 3.0 should require support for multi-person authentication for high-security actions.	We should not shy away from considering insider threats. Of course most election officials are honest and dependable, but we cannot presume that will always be true. People are complicated and can be motivated to act against the security of the system. Recent examples in elections can be found in Michigan, Georgia, and Colorado, where some election officials used their authorized access to facilitate unauthorized access to others. And even an honest insider can lose a key, misplace their access card, or have their password discovered and inadvertently provide an outsider with insider-level access. Multi-party authorization offers stronger security but not without a cost. Getting two people together to enter credentials into a computer can be a burden on election administration. Therefore, it should exist as an optional feature for jurisdictions who want to use it, and it should be reserved for high-security actions, not for routine tasks. Examples of appropriate high-security actions might include making changes to operating system or software accounts or permissions, installing software, changing default settings on optical scanners, enabling adjudication functions, or deleting election data.	Further Investigation required	This is already allowed. It may be a good idea to require capability. Enforcement would be at the Jurisdiction level.	Reject. There are multiple ways of addressing the insider threat such as monitoring and logging capabilities which are found in the VVSG 2.0.	
6/7/23	Free Speech for People	2.0	General	We strongly urge the EAC to reassess and revise the penetration testing provision in the Testing and Certification Manual to effectively utilize this important security tool, and to include requirements that vendors effectively remediate severe security vulnerabilities that are discovered. the penetration testing is not a part of the VVSG 2.0, the tests and results are not public, and there are no requirements to remedy security vulnerabilities that may be uncovered in the process of the penetration testing. In other words, penetration testing may reveal severe security vulnerabilities, but as long as a system conforms to the VVSG 2.0 requirements and test assertions, it can receive full EAC Certification		Reject this proposal, but SECURE IT may mean changes to penetration testing.	Vendors are required to remediate vulnerabilities. Requirements in the manual are required to be followed. SECURE IT act may make changes to this process.	Reject. We agree that the penetration testing needs to be stronger but should be addressed separate from the VVSG requirements.	
6/7/23	Free Speech for People	2.0	General	The VVSG 2.0 should include a provision that prohibits voting system vendors from advertising their products on ballots.		Reject	Jurisdictions are responsible for ballot design and layout.	Agree with EAC decision	

Attachment 1 - 2023 Proposed VVSG Changes

Date	Organization	VVSG	Requirement	Proposed Changes / Additions *Note that red indicates an addition to an existing requirement, and strikethrough indicates removal from an existing requirement.*	Comment / Reasoning	EAC Initial Decision	EAC comment	NIST Initial Decision	NIST Comment
6/21/23	Smartmatic	2.0	General	New CDF standards are being published by NIST. Is there a policy around their inclusion in VVSG?	Recommend establishing an effectivity policy for new CDF's.	Accepted	Only CDFs in the VVSG are required. New CDF publications will need to be added to a future VVSG revision in order to be required.	Agree with EAC decision	
6/7/23	Citizens' Oversight Projects - Ray Lutz	2.0	General	THE FOLLOWING MENTIONS OF E2E VERIFIABLE VOTING SYSTEMSHOULD BE REMOVED FROM THE MAIN BODY OF THE VVSG AND MOVEDTO AN APPENDIX: The following sections are inappropriate for the main body of the VVSG prior to the generation of procedures for evaluation and demonstration of viability It is the opinion of this author that these systems will not be accepted by the public for this application because of the lack of transparency. The unofficial proposals reviewed, as of this time, are far from being sufficiently scalable.		Further Investigation Required	Discussion with other stakeholder concerning E2E required	Agree with EAC decision	
6/7/23	Citizens' Oversight Projects - Ray Lutz	2.0	General	We notice that e-pollbooks, election reporting systems, remote voting systems, ballot printing on-demand are all NOT COVERED by the VVSG. They should be!		Noted	This would require a change to HAVA. EAC ESTEP program is currently developing a pollbook pilot, and will be looking at other VS adjacent systems.	Agree with EAC decision	
6/2/23	National Disability Rights Network	2.0	General	Many certified machines do not provide accessible verification of the printed ballot; they also do not provide automatic paper ballot handling, which threatens the privacy and independence of voters with disabilities casting their ballots and comes with the risk of their ballot becoming separated from the other ballots, which could threaten the secrecy or counting of their ballots.		Noted	VVDG 2.0 does require independent ballot handling. Issues mentioned here are for current systems.	agree with EAC decision	
6/21/23	Voting Works	2.0	General	Increasingly, navigating the VVSG in the format currently available (PDF) is unwieldy and does not take advantage of current practices to make large documents more navigable. It would be useful to have an option to have the VVSG also be provided in a webpage format with tags that enable users to easily jump to sections or specific requirements.		Requires further investigation	Determine if this is wanted / needed.	agree with EAC decision	
6/21/23	Voting Works	2.0	General	With VVSG2 requiring more of voting equipment, notably for accessibility and security, the EAC should follow the lead of all other major standard organizations to prevent this kind of anti-competitive behavior that ultimately harms election administrators and voters. The two important changes that would bring the EAC in line with other standards organizations are: - All EAC-approved vendors should be required to disclose all of their relevant patents. - The EAC should review these patents on a regular basis and, when it determines that such a patent is substantially required to meet the VVSG standard – a so-called essential patent –, should require the vendor to provide a royalty-free license to that patent to other EAC-approved vendors for the narrow purpose of meeting the VVSG standard. A good example of a major standards group patent policy to follow is the W3C's patent policy: https://www.w3. org/Consortium/Patent-Policy-20200915/.		Requires further investigation	This would likely be a question for EAC General Counsel	Agree with EAC decision	
6/7/23	ACM	2.0	General	USTPC endorses the changes proposed to VVSG 2.0 by the State Audit Working Group (SAWG) with regard both to disabling wireless communications and requiring component testing for interoperability.		Reject	See responses to Requirement 14.2	Agree with EAC decision	
6/7/23	ACM	2.0	General	"sunsetting' all earlier versions of the guidelines on a near-term date certain, requiring vendors to certify that all voting systems fully comply with VVSG 2.0, rather than any earlier standard;		Reject	This is outside of scope of VVSG. It's covered in the EAC VVSG Lifecycle Policy	Agree with EAC decision	
6/7/23	ACM	2.0	General	sharply defining what constates a "new system," versus a system "modification;" and		Reject	This is outside of scope of VVSG. It's covered in the EAC VVSG Lifecycle Policy	Agree with EAC decision	
6/7/23	ACM	2.0	General	clarifying that the Commission, not vendors, will make that determination.		Reject	This is outside of scope of VVSG. It's covered in the EAC VVSG Lifecycle Policy	Agree with EAC decision	
6/7/23	ACM	2.0	General	USTPC reiterates its recommendation that recallable ballot use be explicitly and strongly disfavored.		Noted	Disfavored' does not mean banned.	no comment	

Attachment 1 - 2023 Proposed VVSG Changes

Date	Organization	VVSG	Requirement	Proposed Changes / Additions *Note that red indicates an addition to an existing requirement, and strikethrough indicates removal from an existing requirement.*	Comment / Reasoning	EAC Initial Decision	EAC comment	NIST Initial Decision	NIST Comment
6/21/23	Smartmatic	2.0	General	New CDF standards are being published by NIST. Is there a policy around their inclusion in VVSG?	Recommend establishing an effectivity policy for new CDF's.	Accepted	Only CDFs in the VVSG are required. New CDF publications will need to be added to a future VVSG revision in order to be required.	Agree with EAC decision	
6/21/23	Bruce Korb	2.0	General	* All ballots should be scanned * Images of those ballots must be cleaned of any identifying marks, leaving only the votes * The images must be posted to the web site of the relevant election districts * the SHA-512 check sum of each image must be made * these sums must be stored in a file made similarly available * *that* file, in turn, must be summed with the final sum prominently posted on the web site		Reject	This is too prescriptive. All ballots are scanned.	Agree with EAC decision	
6/7/23	Free Speech for People	2.0	Introduction	we recommended adding this sentence to the first paragraph on page 11, “Issues of ballot secrecy can be substantially ameliorated by adopting ballot marking devices that produce a marked paper ballot identical in format and size to pre-printed paper ballots.”		Reject	This is likely overstepping EAC scope, when it comes to system design.	Agree with EAC decision	
6/21/23	Boulder CO Voters	2.0	Introduction	Discussion VVSG uses the following updated interpretation of HAVA Section 301 #3 which accounts for ranked voting, approval voting and score voting: “Notify the voter if they have made an invalid mark, e.g., by selecting or ranking more contest options than allowed, inform the voter of the implications, and provide the voter an opportunity to correct the ballot before it is cast and counted.”		Reject	Requires a change to HAVA., and is outside scope of VVSG.	Agree with EAC decision	
6/7/23	Free Speech for People	2.0	Introduction	In this same section, the VVSG states: “To support best practices, states should consider legislation and additional resources to ensure balanced access to accessible voting machines wherever voting technology is deployed and used for elections.” The VVSG 2.0 should not recommend to legislation to states. This is out of scope for the VVSG and should be deleted.		reject	Best Practices and information sharing is part of EAC scope.	no comment	
8/2/22	Government Blockchain Association	2.0	Principle 1 High-Quality Design	New requirement needs to be added to accommodate remote digital ballot delivery, marking, and return: GBA-WG-1 - All marked ballots and related metadata shall be returned and recorded on a decentralized immutable ledger.		Reject	Out of scope. Remote Delivery, mark and return is outside of Voting Systems.	Reject	out of scope
6/7/23	Free Speech for People	2.0	1.1.2-M (New)	Recommended addition: “1.1.2 M -Logic and accuracy testing functions shall not rely upon any test data stored within the device or subsequently installed electronically into the voting device such as a test pattern.”	This addition is recommended to prevent “auto test” features promoted by vendors which are insufficient and failed to detect programming errors that resulted in incorrect election results in the November 2019 election in Northampton, Pennsylvania.	Accept	EAC is sympathetic to this idea. This would need to be investigated and possibly reworded.	Agree with EAC decision	
8/2/22	Government Blockchain Association	2.0	1.1.3-A – Opening the polls The voting system must provide functions to enter a mode in which voting is permitted.	The below test assertion associated with this requirement specifies scanners and ballot marking devices. This requires modification to accommodate remote digital ballot delivery, marking, and return. TA113A-1: **Scanners and ballot marking devices** MUST provide designated functions for entering voting mode		Reject	Out of VVSG scope. Remote delivery, mark and return is outside of HAVA definition of Voting Systems.	Agree with EAC decision	
6/21/23	Smartmatic	2.0	1.1.4-E, F, K	These are contest types declared (or not) in the system's Implementation Statement. Where VVSG states a "must" in these voting variations, it defeats the purpose of the implementation Statement.	VVSG should be modified to add a comment that the Implementation Statement governs to which voting variations the VSTL will test.	Noted / Reject	This is already covered in the Program Manual, as well as the 'Implementation Statement' section on page 20.	Agree with EAC decision	

Attachment 1 - 2023 Proposed VVSG Changes

Date	Organization	VVSG	Requirement	Proposed Changes / Additions *Note that red indicates an addition to an existing requirement, and strikethrough indicates removal from an existing requirement.*	Comment / Reasoning	EAC Initial Decision	EAC comment	NIST Initial Decision	NIST Comment
6/21/23	Smartmatic	2.0	General	New CDF standards are being published by NIST. Is there a policy around their inclusion in VVSG?	Recommend establishing an effectivity policy for new CDF's.	Accepted	Only CDFs in the VVSG are required. New CDF publications will need to be added to a future VVSG revision in order to be required.	Agree with EAC decision	
3/2/23	Eric Bidstrup, WA Citizen	2.0	1.1.4-J	It can be used for approval voting by setting N equal to M. It can also be used for limited voting by setting N to be less than the number of seats being elected. Approval Voting capabilities must be formally confirmed during testing and certification." to comments	Proponents of Approval Voting interpret the above statements as meaning "If a voting system supports N-of-M contests and has previously been tested and certified as such, that means it is ready to use now without changes or any formal testing for Approval Voting." As the existing VVSG 2.0 text indicates, using N-of-M capabilities and setting N=M is entirely acceptable for Approval Voting contests. However, such an approach is functionally different from limited voting N-of-M contests. Hence why VVSG documents this difference. Assuming that such a difference will work as expected without formal testing and certification creates a situation where it is not formally provable that a voting system indeed does behave correctly for Approval Voting contests. Providing some additional clarification expressing that formally testing Approval Voting by using N-of-M capabilities and setting N=M is required to ensure voter confidence such election systems.	Reject	This is very granular. We disagree that this is 'fundamentally different' Voter confidence in such a scenario would be better served testing at Logic and Accuracy, especially with a public demonstration (if required)	Agree with EAC decision	
6/7/23	Fairvote	2.0	1.1.4-M	Voting system ballot design options should accommodate landscape oriented ballots in the event a contest allows numerous candidate selections so that all or most options and preferences can be displayed on one face of a physical paper ballot when applicable		Reject	Ballot Design and Layout is generally a jurisdiction matter. While landscape might allow for more candidates, there will still be a finite space.	Agree with EAC decision	
5/20/23	State Audit Working Group (SAWG)	2.0	1.1.5-A	**1.1.5-A – Reading ~~Casting~~ and recording** The voting system must support reading ~~casting~~ a ballot, recording each vote precisely as indicated by the voter subject to the rules of the election jurisdiction, and creating and retaining ballot images and ~~a~~ cast vote records that can be tabulated and audited	Comment. In VVSG 2.0 ballot images do not seem to be a requirement for the functionality of voting systems. They seem to be treated as an extension. If ballot images are included as required functionality, then they need to be included in many parts of the VVSG including testing for precision and accuracy, pre-election testing/equipment set-up, recording voter choices, and data protection. This section includes an example of the issues in the misuse of the words "cast" and "ballot" that occur in several places in the guidelines. "Cast" refers to the final act of physically or electronically submitting the ballot, not "reading" which is the actual intent of this section. For each side of a ballot sheet, a separable ballot image is created. For each ballot sheet, a separate cast vote record is created. We have suggested what might be a correct way of stating the requirement.	Reject	A ballot can be read without being cast, e.g. review. So the distinction is important with this requirement "reading a cast ballot". It is a jurisdictional decision for whether to not images of ballots are created and retained.	Agree with EAC decision	
6/7/23	Free Speech for People		1.1.5-B	Recommended Addition: "1.1.5- B An electronic ballot marker may only record contest selections on a paper ballot sheet and may not record, store or export electronic copies of any contest selection."	Electronic ballot markers should not be capable of electronically recording votes; systems which record votes electronically should be classified as Direct Record Electronic.	Reject	1.1.5 -B does not seem to be the relevant requirement for this comment.	Agree with EAC decision	This suggestion is incompatible with other VVSG requirements.
5/20/23	State Audit Working Group (SAWG)	2.0	1.1.5-G	Remove 1 and 2. 4.Identification of the corresponding voted ballot (or ballot sheet if multiple sheets exist);	Comment: A single ballot can consist of multiple styles and multiple sheets. This will affect anonymity because it might prevent more than one ballot style from being assigned to a ballot- thus preventing or making difficult the separation of ballot content into independently tabulated styles. However, if it is made clear that multiple CVRs and multiple styles can be associated with a voter, this problem would be eliminated.	Reject	It is thought that while removing 1 & 2 has the potential to increase voter privacy, it would decrease the ability to audit and diagnose specific devices that might be experiencing anomalies.	Agree with EAC decision	
6/7/23	Verified Voting	2.0	1.1.5-G	We support essentially the current scope of this requirement. In particular, including both "identification of the specific creating device" (often referred to as "tabulator ID") and batch identifiers can be crucial in many tabulation audits and ballot reconciliation processes. Tabulator IDs also can be important in investigating anomalous results.		Noted		Agree with EAC decision	

Attachment 1 - 2023 Proposed VVSG Changes

Date	Organization	VVSG	Requirement	Proposed Changes / Additions *Note that red indicates an addition to an existing requirement, and strikethrough indicates removal from an existing requirement.*	Comment / Reasoning	EAC Initial Decision	EAC comment	NIST Initial Decision	NIST Comment
6/21/23	Smartmatic	2.0	General	New CDF standards are being published by NIST. Is there a policy around their inclusion in VVSG?	Recommend establishing an effectivity policy for new CDF's.	Accepted	Only CDFs in the VVSG are required. New CDF publications will need to be added to a future VVSG revision in order to be required.	Agree with EAC decision	
5/20/23	State Audit Working Group (SAWG)	2.0	1.1.5-H	1.1.5-H – Store and link corresponding image The voting system must ~~be capable of storing~~ store an image of a side or a sheet of a paper ballot and link this image to the specific associated CVR.	Comment: Federal regulation requires that electronic records created must be retained for 22 months.	Reject	As previously mentioned, it is a jurisdiction decision on whether to store images or not.	Agree with EAC decision	
5/20/23	State Audit Working Group (SAWG)	2.0	1.1.5-I - NEW	1.1.5-I -- Ballot Image Hashes, Digital Signatures and Exports The core bit image of each separable unit of the ballot should be hashed to help ensure that any alteration of the image thereafter will be detectable, and the images, when presented in other forms, such as PDF or PNG, can be compared bit-by-bit with the originally scanned image, which was digitally signed by the device. Scanners must provide a means to export the ballot images as separable sheets if not as sides of sheets. Separately, a file containing hashes is created for which a digital signature is also created,	Comment: Tying individual auditable entities to unnecessarily detailed information like the device which generated them can make it impossible to publish the information, and imperil the even more important requirement for transparency of the data. Without transparency, audits are just more unverifiable claims from election officials. This should require hashes of all these individual entities (images etc.), and then require signatures of collections of those hashes in batches which are designed to be safe to release to the public.	Reject	This is covered by 13.2-A - Signing stored election records. Comment is in reference to 1.1.5-G.1 & 2.	Agree with EAC decision	
6/7/23	Free Speech for People		1.1.5-I -NEW	Recommended addition: “Vote choices recorded on paper should be in human readable form.”	Recording vote choices in barcodes creates a non-verifiable record of votes used for counting. Even if the vote choices are also recorded in human readable text, the scanners are counting a record that was not verified by the voter. Even if the election results are robustly audited, studies have shown the voters do not adequately verify the vote selections to provide a reliable audit record. Ballots produced by ballot marking devices should be designed to produce ballots that are identical in format to pre-printed ballots.	Reject	Human readable format are covered in the following requirements: 9.1.3-A - Records for voter verification 9.1.4-A – Auditor verification 9.1.5-B – Paper record retention 9.1.5-C – Paper record intelligibility	Reject	Agree this covered by other requirements.
5/20/23	State Audit Working Group (SAWG)	2.0	1.1.8-A	The voting system must support the tabulation function for all voting variations indicated in the ~~implantation~~ implementation statement. This function includes: 4. delay of aggregation and reporting of any total or partial contest results until close of polls on Election Day.	Scanners shall be able to create ballot images. Steps 1, 2 & 3 may be done in the scanner or Election Management System, and may be delayed until Election Day. Step 4, performing aggregation, shall be delayed until Election Day. That way the votes may be captured and stored early in the process to protect the chain of custody, but the results cannot be easily leaked. While precinct scanners do tabulation and produce poll tapes, they shouldn't be permitted to be used in that way during early voting.	Accepted type, but rejected # 4 as a jurisdictional decision	Agree with typo correction. Recommended addition would likely contradict State laws. These vary between states and is not something that should be enforced via requirements.	Agree with EAC decision	
5/20/23	State Audit Working Group (SAWG)	2.0	1.1.8-H	An N-of-M contest is used for approval voting by setting N to be equal to M. This type of contest is used for limited voting by setting N to be less than the number of seats being elected. Approval Voting capabilities must be formally confirmed during testing and certification.”	Proponents of Approval Voting interpret the above statements as meaning “If a voting system supports N-of-M contests and has previously been tested and certified as such, that means it is ready to use now without changes or any formal testing for Approval Voting.” As the existing VVSG 2.0 text indicates, using N-of-M capabilities and setting N=M is entirely acceptable for Approval Voting contests. However, such an approach is functionally different from limited voting N-of-M contests. Hence why VVSG documents this difference. Assuming that such a difference will work as expected without formal testing and certification creates a situation where it is not formally provable that a voting system indeed does behave correctly for Approval Voting contests. Providing some additional clarification expressing that formally testing Approval Voting by using N-of-M capabilities and setting N=M is required to ensure voter confidence such election systems.	Reject	This is too granular. Voter confidence in such a scenario would be better served testing at Logic and Accuracy, especially with a public demonstration (if required)	Agree with EAC decision	

Attachment 1 - 2023 Proposed VVSG Changes

Date	Organization	VVSG	Requirement	Proposed Changes / Additions *Note that red indicates an addition to an existing requirement, and strikethrough indicates removal from an existing requirement.*	Comment / Reasoning	EAC Initial Decision	EAC comment	NIST Initial Decision	NIST Comment
6/21/23	Smartmatic	2.0	General	New CDF standards are being published by NIST. Is there a policy around their inclusion in VVSG?	Recommend establishing an effectivity policy for new CDF's.	Accepted	Only CDFs in the VVSG are required. New CDF publications will need to be added to a future VVSG revision in order to be required.	Agree with EAC decision	
6/7/23	Fairvote	2.0	1.1.8-J	In order to facilitate tabulation and winner selection across various jurisdictions where different vendor systems may be used, tabulation systems should ensure capture of all relevant data points to ensure interoperability and suability across local election jurisdictions.		Reject	Comment does not reflect the intent of the requirement regarding cumulative voting contests. This is addressed in Principle 4 for interoperability.	Agree with EAC decision	
6/21/23	Boulder CO Voters	2.0	1.1.9-E	The voting system must have the capability to report the number of counted ballots for ~~each relevant N-of-M or cumulative voting~~ contest. Ballot counts should be provided for all contests, regardless of vote variation. ~~The count by contest could be inferred from the other counts that are broken down by ballot configuration, but providing this figure explicitly will make it easier to account for every vote. N-of-M in this requirement includes the most common type of contest, 1-of-M~~		Reject		agree with EAC decision	
6/21/23	Boulder CO Voters	2.0	1.1.9-F	Report votes and percentage support for each contest option All systems must have the capability to report the vote totals for each contest option in each ~~relevant N-of-M or cumulative voting~~ contest and, for multi-round tabulation methods, in each tabulation round. When reporting percentage support for each contest option, systems must calculate the percentage in terms of the number of ballots cast in that contest. Discussion ~~N-of-M in this requirement includes the most common type of contest, 1-of-M.~~In instant runoff voting (IRV), a contest option's vote total may increase, stay the same or decrease to zero in a subsequent round.		Reject / Require further investigation	Percentage calculations are not a requirement. Should they be? Systems do already do this. Will follow up. Reject last comment	Reject. May consider further investigation in the future. It is too soon for this.	
6/7/23	Fairvote	2.0	1.1.9-I	Comment: Transparency and accountability are crucial aspects of the electoral process. System guidelines should promote consistency and ensure that reported results are accessible and understandable to the public.	In order to facilitate optimal speed and transparency in reporting the results of ranked choice contests, particularly for cross-jurisdictional and state-wide contests, we propose the following recommendations for types of data result reporting in ranked contests: - Individual ballot ranking data -Precinct ranking summaries - Cast Vote Record (CVR) & Common Data Format (CDF)	Requires further investigation	This comment seems reasonable. To be researched.	Agree that this needs further research.	It appears there may be ambiguous language that could be cleaned up.
6/7/23	Kevin Skoglund	2.0	1.1.9-K	The title should be changed to "1.1.9-K – No tallies before polls close" and make clear in the text that it applies to all tabulation devices.		Reject	This may conflict with State laws. This would be a jurisdictional decision.	Disagree. This may be an ambiguity if there is a chance that polls open and close before final offical close.	
6/7/23	Free Speech for People	2.0	1.1.9-L	Recommended addition "If ballots are processed in a central-count operation by batch, 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." This will facilitate certain methods of post-election audits.	This will facilitate certain methods of post-election audits.	Requires further investigation	What methods of post-election audits? Are additional requirements necessary to support? Systems do already do this.	Agree with further research.	The current requirement may already allow this.

Attachment 1 - 2023 Proposed VVSG Changes

Date	Organization	VVSG	Requirement	Proposed Changes / Additions *Note that red indicates an addition to an existing requirement, and strikethrough indicates removal from an existing requirement.*	Comment / Reasoning	EAC Initial Decision	EAC comment	NIST Initial Decision	NIST Comment
6/21/23	Smartmatic	2.0	General	New CDF standards are being published by NIST. Is there a policy around their inclusion in VVSG?	Recommend establishing an effectivity policy for new CDF's.	Accepted	Only CDFs in the VVSG are required. New CDF publications will need to be added to a future VVSG revision in order to be required.	Agree with EAC decision	
6/7/23	ACET	2.0	1.2-I	We suggest voting devices must minimally comply with the requirements of the Federal Communications Commission, Part 15, Class A. Hardware compliance to Class B limits is significantly more difficult to achieve, which increases the time for development, testing, and certification. This slows innovation and adoption of new voting system standards and makes voting system acquisition more expensive for jurisdictions while adding little to no value in real-world operating environments. The requirement should be revised to require Class A conformance for all electronic voting devices.	The purpose behind the more stringent requirements for Class B equipment is to reduce the probability that the consumer will need to reposition the device to prevent potential interference with television and radio reception within 30 feet in the home. Not only are voting systems operated in commercial buildings, not homes, but VVSG 2.0 specifically prohibits the use of wireless devices.	Requires further investigation	The FCC definition of Class A and B as it applies to voting devices in typical polling places needs further investigation. The application of Class B here seems to be appropriate based on the idea that the voting devices will frequently be in close proximity to devices like televisions, tablets, and cell phones which necessitates further restriction in emissions. Applicability is not specific to the device in question supporting wireless capability but	Agree with further research.	Since most all hardware that is anticipated to be in VVSG 2.0 systems will be COTS, it will probably all already need class B compliance. Even so, given the ubiiquity of cell phones, class B seems to be needed.
9/28/21	Microvote	2.0	1.2-I – FCC Part 15 Class A and B conformance Voting devices must comply with the requirements of the Rules and Regulations of the Federal Communications Commission, Part 15, Class B [FCC19a]. 1. Voting devices located in polling places must minimally comply with Class B requirements. 2. Voting devices located in non-polling place settings such as back offices must minimally comply with Class A requirements.	Regarding this test assertion: TA12I-2: The voting system documentation MUST indicate whether devices comprising the system are intended to be located in non-polling places (Class A) or polling places (Class B). You delineation of the location (non-polling, polling) does not correspond to the purpose behind the two different standards, which is designed to prevent interference between electronic components in one of two environments: 1. Commercial, industrial, or business 2. Home According to the FCC: Class A digital device. A digital device that is marketed for use in a commercial, industrial or business environment, exclusive of a device which is marketed for use by the general public or is intended to be used in the home. (i) Class B digital device. A digital device that is marketed for use in a residential environment notwithstanding use in commercial, business and industrial environments. Examples of such devices include, but are not limited to, personal computers, calculators, and similar electronic devices that are marketed for use by the general public. The distinguishing factor in the standards has to do with the intended environment for the electronic device. All voting system devices are marketed for use by government entities (not the general public) in conducting elections and intended to be used in commercial, industrial or business environments. Thus ALL voting system devices would be appropriately tested to Class A standards, not Class B. Class A devices are typically home or personal electronics, not voting machines.		Requires further investigation	The FCC definition of Class A and B as it applies to voting devices in typical polling places needs further investigation. The application of Class B here seems to be appropriate based on the idea that the voting devices will frequently be in close proximity to devices like televisions, tablets, and cell phones which necessitates further restriction in emissions. Applicability is not specific to the device in question supporting wireless capability but it's proximity to devices that do such as cell phones.	Agree with further research.	Since most all hardware that is anticipated to be in VVSG 2.0 systems will be COTS, it will probably all already need class B compliance. Even so, given the ubiiquity of cell phones, class B seems to be needed.
8/2/22	Government Blockchain Association	2.0	Principle 2 High Quality Implementation	New requirement needs to be added to accommodate remote digital ballot delivery, marking, and return: GBA-WG-1 - The remote electronic voting application shall transmit the submitted ballot information to an immutable repository and remove the selection data from the memory of the voting selection device.		Reject	Out of scope. Remote Delivery, mark and return is outside of Voting Systems.	Agree with EAC decision	

Attachment 1 - 2023 Proposed VVSG Changes

Date	Organization	VVSG	Requirement	Proposed Changes / Additions *Note that red indicates an addition to an existing requirement, and strikethrough indicates removal from an existing requirement.*	Comment / Reasoning	EAC Initial Decision	EAC comment	NIST Initial Decision	NIST Comment
6/21/23	Smartmatic	2.0	General	New CDF standards are being published by NIST. Is there a policy around their inclusion in VVSG?	Recommend establishing an effectivity policy for new CDF's.	Accepted	Only CDFs in the VVSG are required. New CDF publications will need to be added to a future VVSG revision in order to be required.	Agree with EAC decision	
6/7/23	Kevin Skoglund	2.0	Guideline 2.1	"The voting system and its software are implemented using trustworthy materials and best practices in software development.", the requirements should encourage use of memory safe languages (without requiring them). The discussion section of "2.1-A – Acceptable programming languages" might be an appropriate location.		Requires Further Investigation	This is an interesting thought. EAC will discuss with other stakeholders.	Reject (see also #5)	While memory-safe language usage is encouraged, it alone is not sufficient to ensure memory-safety. Thus, language usage is but one best-practice, but other factors are involved as well. Furthermore, there are many other best practices for implementation. The VVSG is not the appropriate place for implementation guidance.
6/21/23	Smartmatic	2.0	2.1.1-C	The paper specification standard is difficult to use in an elections context.	Perhaps the EAC can select a more mainstream paper specification, or place some minimum paper characteristics directly into VVSG	Accept	EAC agree with this and will investigate paper specifications in the election space.	Agree with EAC decision	
6/7/23	ACET	2.0	2.1.1-C Durability of Paper	The referenced paper characteristics standard is difficult to find and outdated. Perhaps the EAC can select a more mainstream paper specification or place some minimum paper characteristics directly into VVSG 2.0.		Accept	EAC agree with this and will investigate paper specifications in the election space.	Agree with EAC decision	
6/21/23	Smartmatic	2.0	2.1.1-D	Is the "manufacturer" referenced the voting system provider or the paper mill?	clarify the object of this clause	Accept	Will clarify requirement to state that this is Voting System manufacturer	Agree with EAC decision	
8/2/22	Government Blockchain Association	2.0	2.1.2-A – Electronic device maintainability Electronic devices must exhibit the following physical attributes: 1. labels and the identification of test points; 2. built-in test and diagnostic circuitry or physical indicators of condition; and 3. labels and alarms related to failures.	This requires modification to accommodate remote digital ballot delivery, marking, and return. It should be noted that the term "Electric Device" refers to the device controlled by the local election officials that receives and stores the marked ballots. This requirement should be modified to include a verification of the BIOS and Operating system integrity. This should be done regardless of the use of remote electronic devices.		Reject	Out of scope. Remote Delivery, mark and return is outside of Voting Systems.	Agree with EAC decision	
6/21/23	Smartmatic	2.0	2.1.2-B	Here terms such as "easy" and "low" are poor choices for electromechanical system standards. They are not testable.	VVSG should be edited to either quantify or avoid them.	Accept	EAC will investigate and look to quantify or avoid.	Agree with EAC decision	
6/21/23	Smartmatic	2.0	2.1.2-C 3	This clause can be made more clear if tied to a related VVSG clause.	This clause should reference VVSG clause 8.1-K or UL 62368.	Accept		Agree with EAC decision	
6/21/23	Smartmatic	2.0	2.3-C	This clause has a noble intent, but as written is unclear, creates unnecessary restrictions on system architectures, and ultimately reduces the flexibility available through compliant systems for County's to customize results report formats. While maintaining report generation code inside the application/application logic is wise, SQL queries and XSLT have been used securely and reliably for years in voting systems to execute results reporting using templates. Arguably these are now not legal under VVSG 2.0.	This clause could be re-written to clearly allow human reviewable (and VSTL testable) logic inside reporting templates, and disallow self-modifying code as elsewhere specified in VVSG, especially if there is a facility within the voting system to digitally sign report templates.	Requires further investigation	This does not seem unreasonable. EAC will investigate.	Reject	This requirement is a strong b est practice for high quality code.
6/21/23	Smartmatic	2.0	2.3-D	The MITRE reference is useful but does not specifically allow exceptions to this Requirement, such as a hardcoded first use password that the system workflow requires by replaced upon that first use.	A list of allowed examples or similar form of clarification would be good.	Reject	Multiple solutions for first use passwords are possible without hardcoding.	Agree with EAC decision	

Attachment 1 - 2023 Proposed VVSG Changes

Date	Organization	VVSG	Requirement	Proposed Changes / Additions *Note that red indicates an addition to an existing requirement, and strikethrough indicates removal from an existing requirement.*	Comment / Reasoning	EAC Initial Decision	EAC comment	NIST Initial Decision	NIST Comment
6/21/23	Smartmatic	2.0	General	New CDF standards are being published by NIST. Is there a policy around their inclusion in VVSG?	Recommend establishing an effectivity policy for new CDF's.	Accepted	Only CDFs in the VVSG are required. New CDF publications will need to be added to a future VVSG revision in order to be required.	Agree with EAC decision	
8/2/22	Government Blockchain Association	2.0	2.4-A – Modularity 2.4-B – Module testability 2.4-C – Module size and identification 2.5.2-A - Input validation and error defense 2.5.4-J – Memory mismanagement 2.5.4-M – Election integrity monitoring 2.6-A – Surviving device failure 2.6-B – No compromising voting or audit data	These require modification to accommodate remote digital ballot delivery, marking, and return.		Reject	Out of scope. Remote Delivery, mark and return is outside of Voting Systems.	Agree with EAC decision	
6/21/23	Voting Works	2.0	2.5.	EAC should consider adding requirements for accessible remote voting solutions (e.g., accessible electronic ballot) as mail in and vote by mail options increase across the country.		Reject	Out of scope. Remote Delivery, mark and return is outside of Voting Systems.	Agree with EAC decision	
5/20/23	State Audit Working Group (SAWG)	2.0	2.5.1-D	2.5.1-D – Prevent tampering with data All voting devices must prevent access to or manipulation of configuration data, vote data, ballot images and ~~or~~ audit records (for example, by physically tampering with the medium or mechanism containing the data, by other programs on the system, or by faulty code) except where this access is necessary to conduct or verify integrity of the voting process. Also, voting systems must not have "back doors" such as unused ports where an attacker might insert a drive and take over the voting system.		Reject	Covered by requirements: 12.2-C - Physical port restriction 12.2-D - Disabling ports	Agree with EAC decision	
6/7/23	Free Speech for People	2.0	2.5.1-D	Recommended addition: “Voting systems must also not have "back doors" such as bootable USB Drives where an attacker might insert a drive and take over the voting system.”		Reject	Covered by requirements: 12.2-C - Physical port restriction 12.2-D - Disabling ports	Agree with EAC decision	
6/7/23	Kevin Skoglund	2.0	2.5.4	Require manufacturers to document what memory safety measures have been used as part of Requirement 2.5. It is a “nutrition label” approach that allows the manufacturer, the EAC, and Voting System Test Labs to measure a critical security area. The documentation should include what percentage of code is protected by memory safe languages (such as Rust, Go, C#, Java, Swift, Python), by programming techniques and functional audits (e.g., Requirements 2.5.4-H through 2.5.4-K), or through other measures (which must be described).		Requires further investigation	EAC has received questions concerning Rust, and will look to provide an RFI concerning this. This subject requires further investigation. This may be in the discussion area.	Reject.	See previous memory safety responses at 5 and 49
6/7/23	Kevin Skoglund	2.0	2.5.4-H to 2,5.4-K	The text assumes that memory safety will be managed by software developers, not through the design of the programming language. This fact should not be assumed and the Discussion sections should state that memory safe languages are encouraged and their use would satisfy these requirements.		Requires further investigation	EAC has received questions concerning Rust, and will look to provide an RFI concerning this. This subject requires further investigation. This may be in the discussion area.	Reject	Good to encourage memory safe languages but we recognize that their use alone is insufficient to get out of testing since they can be worked around. See also 5 and 49.
6/21/23	Smartmatic	2.0	2.7-H	This clause calls for the voting system to have two hour battery back-up.	Recommend limiting this Requirement to vote capture devices while requiring that all other portions of the voting system have adequate battery to allow for graceful shutdown under conditions such as maximum size batch processing (central count) or ballot generation (election management system).	Accept	This is reasonable - the 2 hour backup is to allow voting to continue in a polling place. It is not so important in a central count / EMS context.	agree with EAC decision	

Attachment 1 - 2023 Proposed VVSG Changes

Date	Organization	VVSG	Requirement	Proposed Changes / Additions *Note that red indicates an addition to an existing requirement, and strikethrough indicates removal from an existing requirement.*	Comment / Reasoning	EAC Initial Decision	EAC comment	NIST Initial Decision	NIST Comment
6/21/23	Smartmatic	2.0	General	New CDF standards are being published by NIST. Is there a policy around their inclusion in VVSG?	Recommend establishing an effectivity policy for new CDF's.	Accepted	Only CDFs in the VVSG are required. New CDF publications will need to be added to a future VVSG revision in order to be required.	Agree with EAC decision	
6/21/23	Smartmatic	2.0	2.7-K	ESD testing requirements - the result requirement, that units withstand ESD discharge "without disruption of normal operation or loss of data" has been a subject of manufacturer-EAC discussion for many years. For example, if the unit reboots and requires a password to re-enter voting (which VVSG 2.0 requires), does that constitute human intervention? This is but one of many areas where the ESD result/behavior requirement is unclear when applied to voting equipment.	Recommend consultation with the VSTLs, third party hardware labs, and Manufacturers to clarify the expectations of equipment undergoing ESD test.	Noted	EAC will look to clarify. Note for EAC testing.	Agree with EAC decision	"Normal" operations should include "normal" human intervention.
8/2/22	Government Blockchain Association	2.0	Principle 3 Transparent	New requirement needs to be added to accommodate remote digital ballot delivery, marking, and return: GBA-WG-2 - The system shall have documented drawings and descriptions that illustrate adherence to applicable standards.		Reject	Out of scope. Remote Delivery, mark and return is outside of Voting Systems.	Agree with EAC decision	
5/20/23	State Audit Working Group (SAWG)	2.0	Principle 3 Transparent	3. System security documentation describes the features of the system that provide or contribute to its security and includes how to operate the system securely. Physical security instructions to protect evidence for both compliance and tabulation audits are included in this documentation. 7.In 3.3, Public documentation requirements cover details of how a manufacturer codes the election event log, implements a CDF, builds barcodes, and supports ~~implements~~ audits.	Manufacturers do not implement audits. They provide systems that provide the data to support audits.	Accept	We agree in principle. EAC should investigate of rewording this.	Agree with EAC decision	
6/7/23	ACET	2.0	3.1.1 -C.9	The requirement to list benchmark directory listings has been in previous VVSG versions and has made its way to VVSG 2.0. While the idea of providing a detailed description of what the system should look like immediately after installation is noble, this requirement results in unusable outputs. When properly implemented on a Windows Server system, the benchmark directory listing is over 27,000 lines of branched directories. It is infeasible for any jurisdiction to review this listing and detect changes, improper or otherwise, to their system. In addition, there may be slight differences in directory listings from jurisdiction to jurisdiction due to hardware variations, further rendering the listing useless to any jurisdiction. This requirement should be removed or significantly modified.		Reject	It has been required in previous versions.	Agree with EAC decision	Automated tools support this.
6/7/23	Free Speech for People	2.0	3.1.1.-E	Recommended addition: "Expected values for confirmed digital signatures of procured software components should be attached to the declaration." A declaration from the manufacturer that software items were obtained directly from the manufacturer or distributor is insufficient. The digital signature and its expected value should be included.		Accept	Accept in Principle, but will look at rewording.	Reject	This is addressed in 3.2-E
8/2/22	Government Blockchain Association	2.0	3.1.1-B – System overview, functional diagram	These require modification to accommodate remote digital ballot delivery, marking, and return. For systems that interface with third-party devices like smart phones, the system documentation must address the third-party devices that are compatible with the system.		Reject	Out of scope. Remote Delivery, mark and return is outside of Voting Systems.	Agree with EAC decision	
5/20/23	State Audit Working Group (SAWG)	2.0	3.1.1-C	10. specifications of the performance and limitations in capacity of the voting system or device,e.g. number of contests, number of contest options per screen, limitations on transition between contests/options/screens etc.	These limitations have caused significant issues in some states. For instance the number of candidates that can be listed on each screen of a BMD should be clear so that all candidates are treated equally.	Reject	Covered by requirements 5.2-A, 7.3-D	Agree with EAC decision	

Attachment 1 - 2023 Proposed VVSG Changes

Date	Organization	VVSG	Requirement	Proposed Changes / Additions *Note that red indicates an addition to an existing requirement, and strikethrough indicates removal from an existing requirement.*	Comment / Reasoning	EAC Initial Decision	EAC comment	NIST Initial Decision	NIST Comment
6/21/23	Smartmatic	2.0	General	New CDF standards are being published by NIST. Is there a policy around their inclusion in VVSG?	Recommend establishing an effectivity policy for new CDF's.	Accepted	Only CDFs in the VVSG are required. New CDF publications will need to be added to a future VVSG revision in order to be required.	Agree with EAC decision	
6/21/23	Smartmatic	2.0	3.1.1-C 9	The requirement to list benchmark directory listings has been in previous VVSG versions and has made its way to VVSG 2.0. While the idea of providing a detailed description of what the system should look like immediately after installation is noble, this requirement results in unusable outputs. When properly implemented on a Windows Server system, the benchmark directory listing is over 27,000 lines of branched directories. It is infeasible for any County to review this listing and detect changes, improper or otherwise, to their system. In addition, there may be slight differences in directory listings from County to County due to hardware variations, further rendering the listing useless to any County.	This requirement should be removed or significantly modified. If it is desired to keep it, consultation with the VSTLs and Manufacturers, possibly around developing a directory delta tool (a software tool that surfaces directory listing differences) would be a sensible approach to making this clause a useful cybersecurity defense measure.	Rejected	This is not a new requirement. I may be possible to look at a directory tool.	Agree with EAC decision	See 68. Automated tools can support this.
6/7/23	Kevin Skoglund	2.0	3.1.2-B	"Maximum tabulation rate", states that "System performance documentation must include the maximum tabulation rate for a bulk-fed scanner. […]".The term "bulk-fed scanner" is not defined in the glossary or used elsewhere in the Requirements. ("Batch-fed scanner" is defined.) More importantly, there is no reason to narrow the scope—it is equally important for manufacturers to provide tabulation rates for voter-facing scanners and E2E-V systems. The text "a bulk-fed scanner" should be changed to "all devices that tabulate" and the discussion section should be changed to match.		Reject	Look at update glossary, but will not include 'all devices'	Agree with EAC decision	
6/7/23	Free Speech for People	2.0	3.1.2-B	Recommended add after section 3.1.2-B "The maximum voting rate for electronic ballot markers (BMD) must be documented to include setup time between voters, time for an average voter to mark a ballot of specified complexity, and the time necessary for an average voter to verify the resulting selections if that must be completed before leaving the BMD."		Reject	Subject to who the voter is and how much time they need. These are not easily averaged/quantified and are not useful.	Agree with EAC decision	
5/20/23	State Audit Working Group (SAWG)	2.0	3.1.2-B	*Change 'tabulation' to 'read and tabulation'. Discussion Add "Scanner processing time must be quoted for a variety of election setup conditions (# contests, # contest options, # sheets, size and layout of sheet, etc.)"		Reject	This will overstep of requirement	Agree with EAC decision	Not sure what the benefit of adding read. Testing should verify that a complex ballot format has a correct throughput rate.
5/20/23	State Audit Working Group (SAWG)	2.0	3.1.2-D	6.After configuration, the system must provide documentation of the current status of any optionally activated capabilities and the parameters associated with them.	For example, one vendor's configuration parameter that is set by hand during election definition and that deserves to be reported back upon request is the range in target pixel density that triggers human adjudication of voter intent on scanned HMPB. The upper and lower bounds of this range are entered at setup time but in some cases are difficult to discover thereafter.	Rejected	Believed to already covered in #5	Agree with EAC decision	
5/20/23	State Audit Working Group (SAWG)	2.0	3.1.3-D	The system security document must include an explanation of how to conduct compliance and tabulation audit procedures to determine whether tabulation is accurate. The explanation should include details such as information about how to locate specific paper ballot sheets from a CVR entry and vice versa, how to export ballot images and CVRs, how to locate and redact rare styles or to redact contests that produce rare styles in coordinated elections.	For information about means to achieve anonymity of CVRs please refer to this article: https://www.sos.state.co.us/pubs/elections/VotingSystems/riskAuditFiles/2018/20180309PreservingAnonymityOfCVR.pdf	Reject	The VVSG are not the place to define how to conduct election audits. While these may be best practices, it is a jurisdictions decision.	Agree with EAC decision	
6/7/23	ES&S	2.0	3.1.4-B	Item 5 states that the software installation documentation must defined as either "application logic, border logic, third party logic, COTS software, or installation software." However, VVSG 2.0 does not include definitions for each software type. The VVSG 1.1 standards provided such definitions and we assume those definitions are still valid but want to confirm. Please include definitions for the following items: application logic, border logic, third party logic, COTS software, or installation software.		Accept	Add missing terms to glossary	Agree with EAC decision	
6/7/23	ACET	2.0	3.1.4-B	Item 5 states that the software installation documentation must be defined as either "application logic, border logic, third party logic, COTS software, or installation software." However, VVSG2.0 does not include definitions for each software type. The VVSG 1.1 standards provided such definitions, and we urge that VVSG 2.0 include them. Otherwise, please confirm the definitions are still valid.		Accept	Add missing terms to glossary	Agree with EAC decision	

Attachment 1 - 2023 Proposed VVSG Changes

Date	Organization	VVSG	Requirement	Proposed Changes / Additions *Note that red indicates an addition to an existing requirement, and strikethrough indicates removal from an existing requirement.*	Comment / Reasoning	EAC Initial Decision	EAC comment	NIST Initial Decision	NIST Comment
6/21/23	Smartmatic	2.0	General	New CDF standards are being published by NIST. Is there a policy around their inclusion in VVSG?	Recommend establishing an effectivity policy for new CDF's.	Accepted	Only CDFs in the VVSG are required. New CDF publications will need to be added to a future VVSG revision in order to be required.	Agree with EAC decision	
6/21/23	Smartmatic	2.0	3.1.6-N	The subject of this clause is not governed by the optical scanner but by paper and ink specifications.	This clause should be incorporated into 3.1.6-M.	Reject	EAC disagrees with this. The two need to be distinguished	no comment	This might benefit from an explanatory discussion. The two are closely related.
6/21/23	Smartmatic	2.0	3.1.6-Q	Due to the highly varied needs of US Counties, these numbers are best normalized. For example, technicians needed per 100 Precinct Count Optical Scanners.	It would be helpful to readers not as familiar with this clause to state in a Discussion box	Reject	EAC would consider an RFI, but as mentioned the varied needs of counties	Agree with EAC decision	
5/20/23	State Audit Working Group (SAWG)	2.0	3.1.7-D	The manufacturer must specify requirements for the orientation and training of administrators, central election officials, election judges, ~~and~~ election workers, equipment maintenance personnel, contractors, and any other individuals who need to interact with the election equipment and/or software.		Reject	"contractors" is too broad here.	Agree with EAC decision	
8/2/22	Government Blockchain Association	2.0	3.2-B – Minimum properties included in the setup inspection process 3.3-B – Specification of Common Data Format	These require modification to accommodate remote digital ballot delivery, marking, and return.		Reject	Out of scope. Remote Delivery, mark and return is outside of Voting Systems.	Agree with EAC decision	
5/20/23	State Audit Working Group (SAWG)	2.0	3.2-R	3.2-R – Accessible election evidence The manufacturer's design must facilitate physical and digital access to all election data including records containing voter intent such as paper ballot sheets, cast vote records, and any ballot images. Discussion The goal should be to ensure constructive sharing and publication of election evidence to support various forms of public verification of the election process. Not all jurisdictions will have the same policies for access but the voting device must support the most transparent of the policies of local officials. Some possible areas of concern include: Records are free of unnecessary links to any voter so that ballot secrecy is maintained, Sometimes voters can be identified if they are voting in a very small contest and/or jurisdiction. The ballots or sheets should be able to be organized so that such information is consolidated into locations such that redaction is inexpensive and quick, and rarely needed. Ballot images may be in convenient storage formats, such as PDF, PNG, and TIF, and other standards. Formats for export are convenient and efficient, and data is well indexed, filterable and sortable. For example, election records are not exported in formats that defy digital or human recognition (e.g., image pdf from which digital text can only be obtained via OCR).	More suggestions about voting system exports to support accessible election evidence are found here: http://electionquality.com/ballot-anonymity-strategies/	Reject	Intent already covered by Principle 3.	Agree with EAC decision	
7/26/23	EAC	2.0	3.3-B	Add references to NIST SP 1500-19 and 1500-20 to discussion.		Accepted		Agree with EAC decision	
5/20/23	State Audit Working Group (SAWG)	2.0	3.3-C	Manufacturers must provide publicly available documentation that fully specifies the barcode, how barcoded data is formatted, and any other encoding standards or methods used on ballots or audit material and allows them to be decoded with COTS devices. (See 4.2-A Standard Formats.) Discussion The voting system documentation needs to include the name and version of the standard used for barcodes or for any other codes that encode information that the public sees on ballots or other material that can be used in audits or verification of the election. The documentation also needs to include how the data may be packed or compressed within the encoding. The report should be sufficient for a voter to understand the barcoded contents and for an auditor to ~~develop applications that~~ examine and fully understand the barcoded contents with minimal need for application development.		Further investigation required	Move test assertions to be part of the requirement. Will need further exploration regarding the use of COTS barcode scanners.	Reject.	Requiring the encoding standard is sufficient for decoding. The request is for the manufacturer to provide the actual decoder program. Some groups may chose to write their own decoders to doublecheck the process. Nothing significant has changed about barcodes since VVSG 2.0

Attachment 1 - 2023 Proposed VVSG Changes

Date	Organization	VVSG	Requirement	Proposed Changes / Additions *Note that red indicates an addition to an existing requirement, and strikethrough indicates removal from an existing requirement.*	Comment / Reasoning	EAC Initial Decision	EAC comment	NIST Initial Decision	NIST Comment
6/21/23	Smartmatic	2.0	General	New CDF standards are being published by NIST. Is there a policy around their inclusion in VVSG?	Recommend establishing an effectivity policy for new CDF's.	Accepted	Only CDFs in the VVSG are required. New CDF publications will need to be added to a future VVSG revision in order to be required.	Agree with EAC decision	
6/7/23	Center for Democracy & Technology	2.0	3.3-C	Manufacturers must provide publicly available documentation that fully specifies the barcode, how barcoded data is formatted, and any other encoding standards or methods used on ballots or audit material. The barcode must be decodable by commercial-off-the-shelf devices. (See 4.2-A – Standard Formats.) Discussion The voting system documentation needs to include the name and version of the standard used for barcodes or for any other codes that encode information that the public sees on ballots or other material that can be used in audits or verification of the election. The documentation also needs to include how the data may be packed or compressed within the encoding. The report should be sufficient for a voter to understand the barcoded contents and for an auditor to ~~develop applications that~~ examine and fully understand the barcoded contents with minimal need for application development.		Further investigation required	Move test assertions to be part of the requirement. Will need further exploration regarding the use of COTS barcode scanners.	Reject	Nothing significant has changed about barcodes since VVSG 2.0
6/7/23	Free Speech for People	2.0	3.3-D	Recommended deletion: "The voting system must be capable of producing a report on an election-by-election basis to show the meaning of codes and other data used within barcodes and CVRs to represent ~~ballot selections and~~ ballot style information." Vote selections should not be encoded in non-human readable form for scanning and counting.		Rejected	Already covered in: TA9.1.5-C 1: If the voting system presents non-human-readable ballot selections (e.g., barcodes or QR codes) THEN they MUST be accompanied by ballot selections presented in a human readable	Reject	Nothing significant has changed about barcodes since VVSG 2.0
9/21/22	NIST	2.0	Principle 4 - Interoperable	Consider any necessary updates to CDF requirements and their impact to the component testing.		Accept	Agree. New CDFs will be reviewed and included as needed.	Agree with EAC decision	
5/20/23	State Audit Working Group (SAWG)	2.0	Principle 4 - Interoperable	The voting system is designed to support interoperability in its interfaces to external systems, its interfaces to internal components, its data, and its peripherals. The voting system and individual voting system components (e.g., EMS, Scanners, BMD) are designed so that individual voting system components can be separately tested and certified. Testing components does not preclude integration testing for entire voting systems.	**The new version of the VVSG should include all requirements necessary to test and certify individual voting system components (EMS, Scanners, BMD …)	Reject	Component testing pilot is in place. This will need to be revisited in the future, following pilot.	Agree with EAC decision	
7/26/23	EAC	2.0	4.1.	Add requirement to include support for CDF for Ballot Definition Specification.	The ballot definition common data format for the interchange of logical and physical ballot style information. Specification can be found in NIST SP 1500-20	Accepted	Requirement language needs to be drafted	agree with EAC decision	
7/26/23	EAC	2.0	4.1.	Add requirement to include support for micro CDF Specification	This is for a data format where environments are space constrained. Specification can be found in NIST SP 1200-19	Accepted	Requirement language needs to be drafted	Agree with EAC decision	
5/20/23	State Audit Working Group (SAWG)	2.0	4.1-A	3.**The ballot definition files must be in a common data format.	Having the election programming data in a common data format is necessary but not sufficient for having true interoperability and testing by component. The ballot definitions themselves must be in a common data format.	Accept	Add micro CDF and ballot definitions.	Agree with EAC decision	
6/7/23	Citizens' Oversight Projects - Ray Lutz	2.0	4.1-C	4.1-C – Exchange of cast vote records (CVRs)", should be amended to allow "exchange of data per the NIST SP 1500-103 Cast Vote Records Common Data Format Specification [CVR_CDF] or equivalent format"	To allow improvement of this format by the market. Calling something the Common Data Format does not make it so, and mandating a wasteful and incomplete format does not help matters. NIST has ceased discussions and does not utilize a consensus-based process.	Reject	Unclear what would be considered equivalent. Having an alternative would undermine the concept of CDF	Agree with EAC decision	
8/2/22	Government Blockchain Association	2.0	4.1-D – Exchange of voting device election event logs	This requires modification to accommodate remote digital ballot delivery, marking, and return. This seems to apply more to the centralized components of remote voting, but should not apply to the devices (i.e., phones) that are used to vote. Separately, we SHOULD encourage that this logging specification offers no immutability protection.		Reject	Out of scope. Remote Delivery, mark and return is outside of Voting Systems.	Agree with EAC decision	
8/2/22	Government Blockchain Association	2.0	4.3-A – Standard device interfaces	This requires modification to accommodate remote digital ballot delivery, marking, and return. This only applies to vendor supplied hardware.		Reject	Out of scope. Remote Delivery, mark and return is outside of Voting Systems.	Agree with EAC decision	

Attachment 1 - 2023 Proposed VVSG Changes

Date	Organization	VVSG	Requirement	Proposed Changes / Additions *Note that red indicates an addition to an existing requirement, and strikethrough indicates removal from an existing requirement.*	Comment / Reasoning	EAC Initial Decision	EAC comment	NIST Initial Decision	NIST Comment
6/21/23	Smartmatic	2.0	General	New CDF standards are being published by NIST. Is there a policy around their inclusion in VVSG?	Recommend establishing an effectivity policy for new CDF's.	Accepted	Only CDFs in the VVSG are required. New CDF publications will need to be added to a future VVSG revision in order to be required.	Agree with EAC decision	
6/21/23	Smartmatic	2.0	4.4-A	This clause creates an obstacle to adoption of COTS hardware in voting systems. Adoption of COTS is a trend across many industries dominated or formerly dominated by purpose built hardware. Many COTS manufacturers test their products using the same tests and test methods as prescribed in VVSG (temperature ranges, shock/vibration, FCC emissions, Radio Frequency Immunity as examples) but typically not to the levels required by VVSG such as 15KV for ESD and 10V/m for RFI).	Re-thinking the philosophy behind this clause and editing it to allow for the Manufacturer to submit data regarding candidate COTS products with subsequent VSTL and EAC technical judgement regarding the goodness of those products would be a more sound approach. It would allow a wider range of COTS products, with associated advantages to the Counties regarding cost and availability.	Reject	All components COTS and proprietary must meet VVSG 2.0 requirements	Agree with EAC decision	
6/7/23	ACET	2.0	4.4-A	This clause creates an obstacle to adoption of COTS hardware in voting systems. Adoption of COTS is a trend across many industries dominated or formerly dominated by purpose-built hardware. Many COTS manufacturers test their products using the same tests and test methods as prescribed in VVSG (temperature ranges, shock/vibration, FCC emissions, Radio Frequency Immunity as examples) but typically not to the levels required by VVSG such as 15KV for ESD. Re-thinking the philosophy behind this clause and editing it to allow for the manufacturer to submit data regarding candidate COTS products with subsequent VSTL and EAC technical judgement regarding the goodness of those products would be a sounder approach. It would allow a wider range of COTS products, with associated advantages to the voting jurisdictions regarding cost and availability.		Reject	All components COTS and proprietary must meet VVSG 2.0 requirements	Agree with EAC decision	
6/7/23	Kevin Skoglund	2.0	Principle 5 and 8	VVSG 3.0 should move the product safety guideline, 8.1, to Principle 2, “High Quality Implementation” and merge the other three guidelines, 8.2-8.4, into Principle 5. The result would be a single principle devoted to requiring voting systems to be accessible as required by HAVA.		Reject		Agree with EAC decision	No rationale provided for why this would be an improvement
8/2/22	Government Blockchain Association	2.0	Principle 5 Equivalent and Consistent Voter Access	New requirement needs to be added to accommodate remote digital ballot delivery, marking, and return. GBA-WG-3 - The system shall authenticate eligible voters who are authorized to submit their ballot electronically.		Reject	Out of scope. Remote Delivery, mark and return is outside of Voting Systems.	Agree with EAC decision	
6/21/23	Voting Works	2.0	5.1-A	In the discussion, it is noted that voters with limited dexterity should be able "to submit their ballots privately and independently without manually handling the ballot." This is not explicit in the requirement and if it is a requirement, it should be explicitly stated.		Accept	This will be incorporated into the requirement.	Accept	it is covered in the requirement, but making it more explicit is OK if that makes it clearer.
8/2/22	Government Blockchain Association	2.0	5.1-A – Voting methods and interaction modes	The test assertions that specifically relate to paper ballot marking do not apply. But the test assertions related to accessibility of electronic ballot marking do apply.		Reject	Out of scope. Remote Delivery, mark and return is outside of Voting Systems.	Agree with EAC decision	
8/2/22	Government Blockchain Association	2.0	Principle 6 Voter Privacy	New requirement needs to be added to accommodate remote digital ballot delivery, marking, and return. GBA-WG-4 – The cast ballot shall not be linkable to the identity of the voter via analysis of information available to any party in the system except the voter himself.		Reject	Out of scope. Remote Delivery, mark and return is outside of Voting Systems.	Agree with EAC decision	
8/2/22	Government Blockchain Association	2.0	Principle 6 Voter Privacy	New requirement needs to be added to accommodate remote digital ballot delivery, marking, and return. GBA-WG-5 - The privacy of the marked ballot is maintained by the system.		Reject	Out of scope. Remote Delivery, mark and return is outside of Voting Systems.	Agree with EAC decision	
6/7/23	Citizens' Oversight Projects - Ray Lutz	2.0	6.2-A	If a voting system includes any features voters might use after casting a ballot as part of end-to-end (E2E) verifiable system ballot tracking, they must be accessible.		Requires further investigation	Discussion with other stakeholder concerning E2E required	Reject	Seems to be covered in 6.2-A.1. Is part of proposed change missing from the spreadsheet?
8/2/22	Government Blockchain Association	2.0	Principle 7 Marked, Verified, and Cast as Intended	New requirement needs to be added to accommodate remote digital ballot delivery, marking, and return. GBA-WG-6 – The voter shall be able to verify their marked ballot as cast.		Reject	Out of scope. Remote Delivery, mark and return is outside of Voting Systems.	Agree with EAC decision	

Attachment 1 - 2023 Proposed VVSG Changes

Date	Organization	VVSG	Requirement	Proposed Changes / Additions *Note that red indicates an addition to an existing requirement, and strikethrough indicates removal from an existing requirement.*	Comment / Reasoning	EAC Initial Decision	EAC comment	NIST Initial Decision	NIST Comment
6/21/23	Smartmatic	2.0	General	New CDF standards are being published by NIST. Is there a policy around their inclusion in VVSG?	Recommend establishing an effectivity policy for new CDF's.	Accepted	Only CDFs in the VVSG are required. New CDF publications will need to be added to a future VVSG revision in order to be required.	Agree with EAC decision	
8/2/22	Government Blockchain Association	2.0	Principle 7 Marked, Verified, and Cast as Intended	New requirement needs to be added to accommodate remote digital ballot delivery, marking, and return. GBA-WG-7 – Prior to casting their ballot, only the eligible voter may mark or revise their ballot selection(s).		Reject	Out of scope. Remote Delivery, mark and return is outside of Voting Systems.	Agree with EAC decision	
8/2/22	Government Blockchain Association	2.0	Principle 7 Marked, Verified, and Cast as Intended	New requirement needs to be added to accommodate remote digital ballot delivery, marking, and return. GBA-WG-8 – The ballot cannot be cast by anyone other than an authenticated user.		Reject	Out of scope. Remote Delivery, mark and return is outside of Voting Systems.	Agree with EAC decision	
8/2/22	Government Blockchain Association	2.0	Principle 7 Marked, Verified, and Cast as Intended	New requirement needs to be added to accommodate remote digital ballot delivery, marking, and return. GBA-WG-9 – The system shall guarantee the recording of the ballot cast as marked.		Reject	Out of scope. Remote Delivery, mark and return is outside of Voting Systems.	Agree with EAC decision	
8/2/22	Government Blockchain Association	2.0	Principle 7 Marked, Verified, and Cast as Intended	New requirement needs to be added to accommodate remote digital ballot delivery, marking, and return. GBA-WG-10 – The system shall guarantee the ballot is recorded as cast.		Reject	Out of scope. Remote Delivery, mark and return is outside of Voting Systems.	Agree with EAC decision	
8/2/22	Government Blockchain Association	2.0	Principle 7 Marked, Verified, and Cast as Intended	New requirement needs to be added to accommodate remote digital ballot delivery, marking, and return. GBA-WG-11 – The system will ensure that only one marked ballot per eligible voter becomes a cast ballot.		Reject	Out of scope. Remote Delivery, mark and return is outside of Voting Systems.	Agree with EAC decision	
8/2/22	Government Blockchain Association	2.0	Principle 7 Marked, Verified, and Cast as Intended	New requirement needs to be added to accommodate remote digital ballot delivery, marking, and return. GBA-WG-12 – Vendors shall adhere to WCAG Version 2.1 level AA and provide the necessary VPAT documentation to prove adherence.		Reject	Out of scope. Remote Delivery, mark and return is outside of Voting Systems.	Agree with EAC decision	
6/21/23	Voting Works	2.0	7.1-D	Understand that these may reflect best practices, but recommend that these options be the default, but that other configurations are allowed to meet a jurisdictions needs. Our organization completed quite a bit of research on this requirement (by talking with accessibility partners) and although we are building to meet this requirement, we have discovered that there are a range of options that would meet the intent of this requirement. These details seem to limit the ability of the manufacturer to provide options for jurisdictions.		Noted	These options must be provided, but other variations are allowed.	Reject (but noted seems fine too)	These requirements were based on significant research for minimum perception.
6/21/23	Voting Works	2.0	7.1-E	Although this requirement generally reflects “best practices”, these requirements are limiting and should not be required. These conflict a bit with the high and low contrast requirements. The requirement could require these to be the default while allowing jurisdictions to change these settings to meet their needs/best practices.		Rejected	There is already a sufficient range.	agree with EAC decision	These requirements were based on significant research for minimum perception.
5/20/23	State Audit Working Group (SAWG)	2.0	7.1-I	The voting system must be capable of printing paper ballots, both ballots for hand marking and BMD printed ballots, that are easily understandable by the voter. Hand marked paper ballots, BMD-printed ballots and other paper records should have ~~with~~ a font size of at least 3.5 mm (10 points). Font and layout on paper should support potential use of optical character recognition on ballot images for use as a means of verification, tabulation, or supplemental audit review.	The VVSG document seems to put much more focus on the usability and readability of the electronic interface than the usability of a hand-marked paper ballot or BMD-printed ballot that the voter is supposed to check. There must be usability testing to see if BMD-printed ballots are printed in such a way to facilitate voters noticing differences between the ballot and their intentions.	Rejected	Easily understandable' is problematic. OCR is already permitted. Hand marked write-ins do not currently work with OCR. EAD will look to take TA5.1-A.4 & 5 and incorporate into VVSG	Agree with EAC decision	
6/7/23	ADT		7.1-I	7.1-I – Text size (paper) The voting system must be capable of printing paper ballots, including blank ballots for hand marking and ballots printed by BMDs, that are easily understandable by the voter. Ballots and other paper records should have a font size of at least 3.5 mm (10 points). Font and layout on paper should support potential use of optical character recognition on ballot images as a means of verification, tabulation, or supplemental audit review.		Rejected	Easily understandable' is problematic. OCR is already permitted. Hand marked write-ins do not currently work with OCR. EAD will look to take TA5.1-A.4 & 5 and incorporate into VVSG	Agree with EAC decision	

Attachment 1 - 2023 Proposed VVSG Changes

Date	Organization	VVSG	Requirement	Proposed Changes / Additions *Note that red indicates an addition to an existing requirement, and strikethrough indicates removal from an existing requirement.*	Comment / Reasoning	EAC Initial Decision	EAC comment	NIST Initial Decision	NIST Comment
6/21/23	Smartmatic	2.0	General	New CDF standards are being published by NIST. Is there a policy around their inclusion in VVSG?	Recommend establishing an effectivity policy for new CDF's.	Accepted	Only CDFs in the VVSG are required. New CDF publications will need to be added to a future VVSG revision in order to be required.	Agree with EAC decision	
6/7/23	Free Speech for People	2.0	7.1-I	Recommended addition: "Font and layout on paper should support potential use of optical character recognition on ballot images for use as an alternative means of tabulation or supplemental audit review." Many ballot marking devices print ballot summary cards with a font size too small for voters to read and verify.		Rejected	Easily understandable' is problematic. OCR is already permitted. Hand marked write-ins do not currently work with OCR. EAD will look to take TA5.1-A.4 & 5 and incorporate into VVSG	Agree with EAC decision	
5/20/23	State Audit Working Group (SAWG)	2.0	7.1-J – Sans-serif font	Add ", Atkinson Hyperlegible " to examples of fonts.	Atkinson Hyperlegible was developed in 2019, so EAC may not be aware of this font. https://brailleinstitute.org/freefont	Accept	Will be added.	Agree with EAC decision	it is a free san-serif font for general use, so we can add it as an example.
8/2/22	Government Blockchain Association	2.0	7.1-N – Tactile keys	This requires modification to accommodate remote digital ballot delivery, marking, and return. These requirements seem to apply to vendor-supplied hardware.		Reject	Out of scope. Remote Delivery, mark and return is outside of Voting Systems.	Agree with EAC decision	
8/2/22	Government Blockchain Association	2.0	7.2-A – Display and interaction options	This requires modification to accommodate remote digital ballot delivery, marking, and return. These requirements seem to apply to vendor-supplied hardware.		Reject	Out of scope. Remote Delivery, mark and return is outside of Voting Systems.	Agree with EAC decision	
6/7/23	Fairvote	2.0	7.2-C.5	Comment: To maintain the integrity and clarity of ballots, we strongly support the requirement that ballots with preferential or ranking voting methods must not reorder candidates except in response to an explicit voter command. This requirement helps to prevent confusion and ensures that the marking of selections remains consistent across contests. Automatic reordering could become a barrier for voters with physical or cognitive disabilities as well.		Noted		Agree with EAC decision	
6/21/23	Voting Works	2.0	7.2-E	Have some concerns that these will change over time, just as they have in the past. Faced similar problems with 1.0 when suddenly touchscreen smartphones came out and people were using touchscreens in much different ways than they did in the years and decades prior to touchscreen phones and tablets. This should be reviewed each year VVSG is reviewed to be sure that it is expansive enough to accommodate changes in available tech.		Noted	VVSG reviews and updates are occurring more frequently than they did with 1.0	Agree with EAC decision	
8/2/22	Government Blockchain Association	2.0	7.2-E – Touch screen gestures	This requires modification to accommodate remote digital ballot delivery, marking, and return. For remote voting, the election system vendor is responsible for supporting accessibility features that are native to the user's device.		Reject	Out of scope. Remote Delivery, mark and return is outside of Voting Systems.	Agree with EAC decision	

Attachment 1 - 2023 Proposed VVSG Changes

Date	Organization	VVSG	Requirement	Proposed Changes / Additions *Note that red indicates an addition to an existing requirement, and strikethrough indicates removal from an existing requirement.*	Comment / Reasoning	EAC Initial Decision	EAC comment	NIST Initial Decision	NIST Comment
6/21/23	Smartmatic	2.0	General	New CDF standards are being published by NIST. Is there a policy around their inclusion in VVSG?	Recommend establishing an effectivity policy for new CDF's.	Accepted	Only CDFs in the VVSG are required. New CDF publications will need to be added to a future VVSG revision in order to be required.	Agree with EAC decision	
6/7/23	ES&S	2.0	7.2-N	We agree that voters must have fast response times from the voting system. By design, we artificially delay some responses to avoid inadvertent double-taps. Based on our experience, slightly longer visual responses can help voters. Also these timings may increase the cost of the system in order to support them. Previously the requirements for 3 second response requirements were sufficient and easier to maintain during the life of a product. Specifically, the timings for item 1.a and 1.b are significantly more burdensome than past requirements and will be difficult to test to these standards. Please clarify how the visual change time requirement will be tested and measured. As written, this requirement could result in obsolescence of currently deployed systems. The introduction of this new standard could prove to be onerous and cost prohibitive for election officials as they will be required to purchase new systems. Our previous request for changes to this section were accepted but no changes were made to the final requirement. This requirement's first sentence needs to be changed to "should" rather than a "must." Revise the requirement to: "The voting system's response time should meet the following standard response times: 1. The system initially responds to a voter action in no more than: a. 0.1 seconds for a visual change b. 0.5 seconds for an audio change 2. The system responds to a voter marking a vote in no more than 1 second for both a visual response and an initial audio response 3. The system completes the visual response or display in no more than 1 second or displays an indicator that a response is still being prepared." This requirement shall only apply to new products introduced into certification testing for the first time.		Reject	Requirement will stay as MUST without a double standard	Agree with EAC decision	
6/7/23	ACET	2.0	7.2-N	Revise the requirement to: "The voting system's response time should meet the following standard response times: 1. The system initially responds to a voter action in no more than: a. 0.1 seconds for a visual change. b. 0.5 seconds for an audio change. 2. The system responds to a voter marking a vote in no more than 1 second for both a visual response and an initial audio response. 3. The system completes the visual response or display in no more than 1 second or displays an indicator that a response is still being prepared." This requirement shall only apply to new products introduced into certification testing for the first time.	We agree that voters must have fast response times from the voting system. By design, we artificially delay some responses to avoid inadvertent double-taps. Based on our experience, slightly longer visual responses can help voters. Also, these timings may increase the cost of the system in order to support them. Previously the requirements for 3-second response requirements were sufficient and easier to maintain during the life of a product. Specifically, the timings for items 1.a and 1.b are significantly more burdensome than past requirements and will be difficult to test to these standards. Please clarify how the visual change in time will be tested and measured. As written, this requirement could result in obsolescence of currently deployed systems. The introduction of this new standard could prove to be onerous and cost prohibitive for election officials as they will be required to purchase new systems.	Reject	Requirement will stay as MUST without a double standard	Agree with EAC decision	
6/7/23	Verified Voting	2.0	7.3-G	For BMD marked ballots, the VVSG should explicitly require the voting system to prompt the voter to check their printed ballot before casting it. (Additional voting system support for voter verification may be warranted.) This requirement could be added to 7.3-G or included separately, as follows: "[the electronic voting interface] prompts the voter to review their printed ballot for correctness before casting it."		Accept	Wording will be deliberated on and added to the requirement.	Agree with EAC decision	yes, a good addition; should discuss if "prompt" is the word to use or perhaps "instruct" or "direct"
6/7/23	ADT		7.3-H	7.3-H – Voter verification of BMD-printed ballots A BMD must inform the voter that the printed paper ballot is the official record of their vote and that the voter should verify the BMD-printed ballot before casting it. Discussion This requirement is intended to increase the likelihood that a voter will verify that their printed ballot reflects their intended choices, before they cast it.		Reject	Jurisdiction requirement to determine what is considered an official record. It cannot be made as a federal level requirement.	Agree with EAC decision	

Attachment 1 - 2023 Proposed VVSG Changes

Date	Organization	VVSG	Requirement	Proposed Changes / Additions *Note that red indicates an addition to an existing requirement, and strikethrough indicates removal from an existing requirement.*	Comment / Reasoning	EAC Initial Decision	EAC comment	NIST Initial Decision	NIST Comment
6/21/23	Smartmatic	2.0	General	New CDF standards are being published by NIST. Is there a policy around their inclusion in VVSG?	Recommend establishing an effectivity policy for new CDF's.	Accepted	Only CDFs in the VVSG are required. New CDF publications will need to be added to a future VVSG revision in order to be required.	Agree with EAC decision	
6/7/23	Florida Fair Elections Coalition		7.3-H	As a result of our studies, which can be found at the following links, we believe that the ballot should be physically kicked back to the voter, allowing them time to realize there is an error on their ballot, understand what the error is, understand that they will lose their vote in the overvoted race if it is not corrected, and time to correct that error. Simply notifying the voter on a screen does not adequately protect against overvotes on optical and digital scan voting machines.		Reject	Update related requirements to include 1.1.6-D	Agree with EAC decision	
5/20/23	State Audit Working Group (SAWG)	2.0	7.3-II (Should be 7.3-Q)	7.3-II - Voter verification of BMD-printed ballots A voting system with an electronic interface must inform the voter that the paper ballot is the official record of their vote and that the voter should check the BMD- printed ballot before casting it. The voting system must be evaluated for usability by voters both in terms of the rate at which voters thoroughly review their ballots and in terms of how successful voters are in discovering any discrepancies between the ballot and their intended selections	Studies have shown that few voters actually verify their BMD-printed ballot. [Insertion of this section requires renumbering.]	Reject	Jurisdiction requirement to determine what is considered an official record. It cannot be made as a federal level requirement.	Agree with EAC decision	
8/2/22	Government Blockchain Association	2.0	7.3-K – Warnings, alerts, and instructions	This requires modification to accommodate remote digital ballot delivery, marking, and return.		Reject	Out of scope. Remote Delivery, mark and return is outside of Voting Systems.	Agree with EAC decision	
8/2/22	Government Blockchain Association	2.0	7.3-M – Identifying languages	This requires modification to accommodate remote digital ballot delivery, marking, and return.		Reject	Out of scope. Remote Delivery, mark and return is outside of Voting Systems.	Agree with EAC decision	
8/2/22	Government Blockchain Association	2.0	7.3-O – Instructions for election workers	This requires modification to accommodate remote digital ballot delivery, marking, and return.		Reject	Out of scope. Remote Delivery, mark and return is outside of Voting Systems.	Agree with EAC decision	
6/21/23	Voting Works	2.0	7.3-P	This references best practices but does not identify the source of said best practices.		Noted	While the best practices comes from a variety of discussions and organizations, including NIST, they are outlined in the discussion.	Agree with EAC decision	
5/20/23	State Audit Working Group (SAWG)	2.0	Principle 8	8.4 - The voting system is evaluated for usability for the role of ~~with~~ election workers.		Reject	Requires the use of election workers in testing, as opposed to role players.	Agree with EAC decision	

Attachment 1 - 2023 Proposed VVSG Changes

Date	Organization	VVSG	Requirement	Proposed Changes / Additions *Note that red indicates an addition to an existing requirement, and strikethrough indicates removal from an existing requirement.*	Comment / Reasoning	EAC Initial Decision	EAC comment	NIST Initial Decision	NIST Comment
6/21/23	Smartmatic	2.0	General	New CDF standards are being published by NIST. Is there a policy around their inclusion in VVSG?	Recommend establishing an effectivity policy for new CDF's.	Accepted	Only CDFs in the VVSG are required. New CDF publications will need to be added to a future VVSG revision in order to be required.	Agree with EAC decision	
6/7/23	ACET	2.0	8.1-A	Regarding the following: 1. For all electronic display screens: a. Antiglare screen surface that shows no distinct virtual image of a light source or a means of physically shielding the display from such reflections, and b. Minimum uniform diffuse ambient contrast ratio for 500 lx illuminance: 10:1. 2. If the display is the primary visual interface for making vote selections: a. Minimum diagonal display size: 12 inches, and b. Minimum display resolution: 1920 x 1080 pixels. 3. If the display screen is for messages to voters or poll workers: a. Minimum diagonal display size: 7.9 inches, and b. Minimum display resolution: 1024 x 768 pixels. We urge EAC to strike this requirement as it does not meet the intent of the 8.1 guideline, and it focuses on technical specifications of components (which is prescriptive) and not the legibility of text (which is the performance metric that should be used). Those performance metrics are already covered by other requirements, such as 7.1-G Text size (electronic display). As an additional point for striking Requirement 8.1-A, the display contrast ratio is listed in 8.1-A(1b), but it is already defined in Requirement 7.1-C, so having the contrast requirement also listed in 8.1-A is not necessary.	The items listed in Requirement 8.1-A do not qualify as elements that would expose users to harmful conditions, and the robustness of a display is not measured in screen size and pixel resolutions. It should be understood that displays on voting systems provide text, lines, and icons (checkmarks, arrows, etc.). Voting systems are not meant to be displaying high resolution photographs or movie videos. Although some LCD panels that are commercially available today have 1920x1080 resolutions, that does not mean that voting systems require those resolutions to display their intended content (text, lines and icons). To display a text character (A, B, 2, etc.), one can universally use a 5x7 pixel matrix. What matters is how small that text can get before it becomes illegible. If a 5x7 pixel matrix is used to display characters on a high-resolution screen, those characters would not be legible, but if that same 5x7 pixel matrix is used to display characters on a low-resolution screen, those characters would be legible. In voting systems, text size should be the major concern, not pixel resolution on displays. The text size will dictate the number of characters that can be legibly displayed across that screen, so screen size is dependent on the amount of text that is intended to be displayed legibly across that screen. If a ballot is being laid out on a display, and there is a large number of candidates or lines of text to describe a bond question or constitutional issue, then a larger screen is needed to properly display that information. But if the device is just providing a message to the voter that "Your ballot was cast!" or "Overvote detected in Contest-Attorney General", then a diagonal screen size of 7.9 inches is not needed to display that content. A device only needs a screen size and pixel resolution that can legibly fit the text that device is intended to display. To provide requirements for screen sizes, resolutions, and pixel counts is technically specific and prescriptive. The focus should be on text sizes and legibility requirements so that the devices can be designed to use the appropriate screen sizes and pixel resolutions for the content they are intended to display. The text sizes are already provided in Requirement 7.1-G,	Requires Further Investigation	Reach out to NIST to understand the resolution display minimum. Reject the notion that a smaller screen can be used with limiting the messaging that a device displays. Review screens should be available on all precinct scanners to meet in 9.1.3-A	Reject. Ideally, it is the legibility that is important, but legibility is very difficult to test as a performance metric. The intent of this requirement is to set a baseline for robust displays that will support good legibility for voters. It was developed by the EAC-NIST working group with input from experts and the manufacturers. Considerations included that display sizes and characteristics were readily available in the COTS marketplace. The req. ensures that a inadequate display will not be deployed. In the future, we are open to specific amendments to the	NIST recommends rejecting this as it in impractical to do this with a straight performance requirment. Having some specificiations is practical.
6/21/23	Dominion	2.0	8.1-A	Strike this requirement as it does not meet the intent of the 8.1 guideline and it focuses on technical specifications of components (which is prescriptive) and not the legibility of text (which is the performance metric that should be used). Those performance metrics are already covered by other requirements, such as "7.1-G Text size (electronic display)".		Requires Further Investigation	Reach out to NIST to understand the resolution display minimum. Reject the notion that a smaller screen can be used with limiting the messaging that a device displays. Review screens should be available on all precinct scanners to meet in 9.1.3-A	Reject	see prior comment on 135
6/7/23	ACET	2.0	8.1-I	Cycles for VVSG approval are long (and it is good that the new annual review process provides some relief for this) and it is possible that 3.5mm jacks are not what a number of today's PAT devices are using for input/output. PAT is aligned with iOS controls, mouse emulation, joystick emulation and other modes -- but these require USB-A connectivity. We believe the EACshould research this clause in VVSG 2.0 for continued relevance in addressing PAT evolution.		Reject	Having USB-A ports available may well lead to security vulnerabilities.	Agree with EAC decision	
6/21/23	Voting Works	2.0	8.3-A	Usability testing - This testing, which is required as part of the TRR, is mentioned at a high level, but specifically outlined in the test assertions. We assume the details are in the test assertions so that they can be easily updated, but the more logical place for the details would be in the VVSG itself or in the Program Manual, in the section that relates to the TRR. Commenter requests that the EAC consider expanding the depth of this requirement in VVSG and adds more detail about this testing to the VVSG and the Program manual.		Reject	It's not part of the TRR and refers to SO/IEC 25062/2006	Agree with EAC decision	

Attachment 1 - 2023 Proposed VVSG Changes

Date	Organization	VVSG	Requirement	Proposed Changes / Additions *Note that red indicates an addition to an existing requirement, and strikethrough indicates removal from an existing requirement.*	Comment / Reasoning	EAC Initial Decision	EAC comment	NIST Initial Decision	NIST Comment
6/21/23	Smartmatic	2.0	General	New CDF standards are being published by NIST. Is there a policy around their inclusion in VVSG?	Recommend establishing an effectivity policy for new CDF's.	Accepted	Only CDFs in the VVSG are required. New CDF publications will need to be added to a future VVSG revision in order to be required.	Agree with EAC decision	
6/7/23	ADT		8.3-A	The manufacturer must conduct usability tests with voters using the voting system., ~~including all voter activities in a voter session from ballot activation to verification and casting.~~ ~~The test participants must include voters who represent the following:~~ ~~1. General population, using the visual interface (without audio), including:~~ 1. The test participants must include: a. voters using the visual interface without the audio format; b. voters who are native speakers of the language being tested for each language defined as supported in the technical data package (TDP); c. blind voters, using the audio format plus tactile controls; d. voters with low vision, using the enhanced visual features with and without audio; and e. voters with limited dexterity, using the visual interface with low and no dexterity controls 2. Usability tests must include all voter activities in a voter session from ballot activation to verification and casting. 3. Usability tests for ballot marking devices (BMDs) must evaluate the percentage of voters who review their ballots and the frequency with which they detect discrepancies between their intended selections and the human-readable information printed on the ballot. 4. The manufacturer must submit a report of the results of their usability tests, including effectiveness, efficiency, and satisfaction measures, as part of the TDP using ISO/IEC 25062:2006: Common Industry Format (CIF) for Usability Test Reports [ISO06b].		Accept the working of #1, Reject the remainder	" Evaluate the percentage of voters who review their ballots" is reviewing the voters, not the system. This also assumes that there are discrepancies in the barcode. Barcode's are covered in principles 3 and 9.	reword EAC comment "Reject the "remainder labelled #3". just to be precise. We don't want to lose #2	
6/7/23	Verified Voting	2.0	8.3-A	Paper record usability testing should be explicitly mandated under this requirement and the associated test assertions, for instance, adding the following the introductory text in 8.3-A: "Usability tests must include testing of the voter verified paper records produced by the voting system."	This requirement implies that paper records produced by paper-based voting systems must be included in the usability testing (as part of "all voter activities in a voter session from ballot activation to verification and casting"). However, neither the requirement and discussion nor the test assertions specifically address testing voters' ability to verify the voter verified paper records. This is a serious omission. It is crucial to ensure that voters with all the various characteristics mentioned in 8.3-A can, in realistic conditions, verify their VVPRs before casting. Nominally voter-verifiable paper records that many voters cannot verify in practice, due to design flaws in the equipment or the records themselves, do not provide substantive software independence.	Reject	Ballot Layout is up to the jurisdiction's laws / policies. 'All activities' is inclusive of digital and paper.	Agree with EAC decision	
6/7/23	Free Speech for People	2.0	8.3-A	Recommended adding point “3. In particular, they must report the rate at which voters detect and report discrepancies with BMD printed ballots purposely misprinted during the usability test.” News reports indicate voters have found errors in the printed ballot summary produced by a BMD. It’s essential to also track such errors in usability tests.		Reject	This seems like an L&A test for usability testing. "errors in the printed ballot summary produced by a BMD" assumes issues are with the BMD.	Agree with EAC decision	
8/2/22	Government Blockchain Association	2.0	8.3-A – Usability tests with voters The manufacturer must conduct usability tests with voters using the voting system, including all voter activities in a voter session from ballot activation to verification and casting.	The following test assertion associated with this requirement needs to be modified. Unsure whether this means braille or could simply mean Voice-over, talkback and screen reader navigation. Needs clarification. TA83A-7: Test participants MUST include blind voters using tactile controls.		Reject	Out of scope. Remote Delivery, mark and return is outside of Voting Systems.	Agree with EAC decision	

Attachment 1 - 2023 Proposed VVSG Changes

Date	Organization	VVSG	Requirement	Proposed Changes / Additions *Note that red indicates an addition to an existing requirement, and strikethrough indicates removal from an existing requirement.*	Comment / Reasoning	EAC Initial Decision	EAC comment	NIST Initial Decision	NIST Comment
6/21/23	Smartmatic	2.0	General	New CDF standards are being published by NIST. Is there a policy around their inclusion in VVSG?	Recommend establishing an effectivity policy for new CDF's.	Accepted	Only CDFs in the VVSG are required. New CDF publications will need to be added to a future VVSG revision in order to be required.	Agree with EAC decision	
8/2/22	Government Blockchain Association	2.0	8.3-A – Usability tests with voters The manufacturer must conduct usability tests with voters using the voting system, including all voter activities in a voter session from ballot activation to verification and casting.	The following test assertion associated with this requirement needs to be modified. TA83A-7-1: The visual acuity of these test participants MUST be less than 20/200 OR these participants MUST NOT be able to use the low-vision interface.		Reject	Out of scope. Remote Delivery, mark and return is outside of Voting Systems.	agree with EAC decision	
8/2/22	Government Blockchain Association	2.0	8.3-A – Usability tests with voters The manufacturer must conduct usability tests with voters using the voting system, including all voter activities in a voter session from ballot activation to verification and casting.	The following test assertion associated with this requirement needs to be modified. Needs clarification. TA83A-13: The population under test SHOULD NOT consist of voters who have previously participated in a voting system usability test.		Reject	Out of scope. Remote Delivery, mark and return is outside of Voting Systems.		
8/2/22	Government Blockchain Association	2.0	8.3-A – Usability tests with voters The manufacturer must conduct usability tests with voters using the voting system, including all voter activities in a voter session from ballot activation to verification and casting.	The following test assertion associated with this requirement needs to be modified. TA83A-18: The manufacturer SHOULD note any differences between the users profiled as recruits and the users who participated in the actual study.		Reject	Out of scope. Remote Delivery, mark and return is outside of Voting Systems.	Agree with EAC decision	
8/2/22	Government Blockchain Association	2.0	8.3-A – Usability tests with voters The manufacturer must conduct usability tests with voters using the voting system, including all voter activities in a voter session from ballot activation to verification and casting.	The following test assertion associated with this requirement needs to be modified. Recommended, not mandatory. TA83A-20: The manufacturer SHOULD ensure that at least 30 test participants are able to complete the testing session.		Reject	Out of scope. Remote Delivery, mark and return is outside of Voting Systems.	Agree with EAC decision	

Attachment 1 - 2023 Proposed VVSG Changes

Date	Organization	VVSG	Requirement	Proposed Changes / Additions *Note that red indicates an addition to an existing requirement, and strikethrough indicates removal from an existing requirement.*	Comment / Reasoning	EAC Initial Decision	EAC comment	NIST Initial Decision	NIST Comment
6/21/23	Smartmatic	2.0	General	New CDF standards are being published by NIST. Is there a policy around their inclusion in VVSG?	Recommend establishing an effectivity policy for new CDF's.	Accepted	Only CDFs in the VVSG are required. New CDF publications will need to be added to a future VVSG revision in order to be required.	Agree with EAC decision	
8/2/22	Government Blockchain Association	2.0	8.3-A – Usability tests with voters The manufacturer must conduct usability tests with voters using the voting system, including all voter activities in a voter session from ballot activation to verification and casting.	The following test assertion associated with this requirement needs to be modified. Recommended, not mandatory. TA83A-21: The manufacturer SHOULD include detailed tables of all participant demographics, whether or not they completed the test, as an appendix to the test report.		Reject	Out of scope. Remote Delivery, mark and return is outside of Voting Systems.	Agree with EAC decision	
8/2/22	Government Blockchain Association	2.0	8.3-A – Usability tests with voters The manufacturer must conduct usability tests with voters using the voting system, including all voter activities in a voter session from ballot activation to verification and casting.	The following test assertion associated with this requirement needs to be modified. Recommended, not mandatory. TA83A-22-1: The manufacturer SHOULD use the Modified CIF Template for manufacturers as a template and guidance for the semantics, content and testing.		Reject	Out of scope. Remote Delivery, mark and return is outside of Voting Systems.	Agree with EAC decision	
8/2/22	Government Blockchain Association	2.0	8.3-A – Usability tests with voters The manufacturer must conduct usability tests with voters using the voting system, including all voter activities in a voter session from ballot activation to verification and casting.	The following test assertion associated with this requirement needs to be modified. TA83A-26: The test ballot used in the usability tests SHOULD look like a real ballot, such as the NIST test ballot.		Reject	Out of scope. Remote Delivery, mark and return is outside of Voting Systems.	Agree with EAC decision	
8/2/22	Government Blockchain Association	2.0	8.4-A – Usability tests with election workers The manufacturer must conduct usability tests of the voting system setup, operation during voting, and shutdown as documented by the manufacturer, with representative election workers, to demonstrate that election workers can learn, understand, and perform these tasks successfully.	The following test assertion associated with this requirement needs to be modified. Could "election worker" here refer to election official using admin console from their office? TA84A-1: The documentation required for normal voting system operation MUST be presented at a level appropriate for election workers who are not experts in voting system and computer technology.		Reject	Out of scope. Remote Delivery, mark and return is outside of Voting Systems.	Agree with EAC decision	

Attachment 1 - 2023 Proposed VVSG Changes

Date	Organization	VVSG	Requirement	Proposed Changes / Additions *Note that red indicates an addition to an existing requirement, and strikethrough indicates removal from an existing requirement.*	Comment / Reasoning	EAC Initial Decision	EAC comment	NIST Initial Decision	NIST Comment
6/21/23	Smartmatic	2.0	General	New CDF standards are being published by NIST. Is there a policy around their inclusion in VVSG?	Recommend establishing an effectivity policy for new CDF's.	Accepted	Only CDFs in the VVSG are required. New CDF publications will need to be added to a future VVSG revision in order to be required.	Agree with EAC decision	
8/2/22	Government Blockchain Association	2.0	8.4-A – Usability tests with election workers The manufacturer must conduct usability tests of the voting system setup, operation during voting, and shutdown as documented by the manufacturer, with representative election workers, to demonstrate that election workers can learn, understand, and perform these tasks successfully.	The following test assertion associated with this requirement needs to be modified. Needs clarification. TA84A-1-1: The documentation SHOULD NOT presuppose familiarity with personal computers.		Reject	Out of scope. Remote Delivery, mark and return is outside of Voting Systems.	Agree with EAC decision	
8/2/22	Government Blockchain Association	2.0	8.4-A – Usability tests with election workers The manufacturer must conduct usability tests of the voting system setup, operation during voting, and shutdown as documented by the manufacturer, with representative election workers, to demonstrate that election workers can learn, understand, and perform these tasks successfully.	The following test assertion associated with this requirement needs to be modified. TA84A-19: The manufacturer MUST ensure that the election workers usability documentation/report is included in the TDP.		Reject	Out of scope. Remote Delivery, mark and return is outside of Voting Systems.	Agree with EAC decision	
6/7/23	Citizens' Oversight Projects - Ray Lutz	2.0	Principle 9	1 - Software independence requires that the voting system provide software independent proof that the ballots have been recorded correctly ~~and are compliant within the Paper-based System Architecture or Cryptographic E2E System Architectures.~~ 6 - Deleted entirely		Require further investigation.	Discussion with other stakeholder concerning E2E required	Accept	This seems reasonable for the overview section.
8/2/22	Government Blockchain Association	2.0	Principle 9 Auditable	New requirement needs to be added to accommodate remote digital ballot delivery, marking, and return. GBA-WG-13 The system shall immutably record: 1) the voter selection for each question in the election. 2) Timestamp 3) Jurisdiction or precinct & ballot style 4) Data linking the cast ballot to the immutable ledger. 5) Data that allows the voter to anonymously and confidentiality verify their vote is cast as intended and recorded as cast.		Reject	Out of scope. Remote Delivery, mark and return is outside of Voting Systems.	Agree with EAC decision	Agree with EAC. Out of scope.

Attachment 1 - 2023 Proposed VVSG Changes

Date	Organization	VVSG	Requirement	Proposed Changes / Additions *Note that red indicates an addition to an existing requirement, and strikethrough indicates removal from an existing requirement.*	Comment / Reasoning	EAC Initial Decision	EAC comment	NIST Initial Decision	NIST Comment
6/21/23	Smartmatic	2.0	General	New CDF standards are being published by NIST. Is there a policy around their inclusion in VVSG?	Recommend establishing an effectivity policy for new CDF's.	Accepted	Only CDFs in the VVSG are required. New CDF publications will need to be added to a future VVSG revision in order to be required.	Agree with EAC decision	
9/21/22	NIST	2.0	Principle 9 Introduction	6 - Cryptographic E2E verifiable deals with cryptographic protocols used in cryptographic E2E verifiable (not paper-based) voting systems, requiring that they be publicly available for review ~~for 2 years~~ before being used in a voting system. Individuals who vote on a cryptographic E2E verifiable system will get a receipt and be able to confirm that the system correctly interpreted 180 Requirements for VVSG 2.0 February 10, 2021 their ballot selections. Voters will also be able to verify that their ballots are included in the tabulation results.		Accept	Requires review of language.	Agree with EAC decision	NIST Submitted comment
6/7/23	Citizens' Oversight Projects - Ray Lutz	2.0	9.1.	An error or fault in the voting system software or hardware, or malicious change in the data, cannot cause an undetectable change in election results.		Accept	Propose "An error, fault, or change in the voting system software or hardware, cannot cause an undetectable change in election results". Changes don't need to be malicious. This is used at several points in VVSG.	Reject	The comment is recommending a change to the Principle and may not be describing a change to the software/hardware but rather to the election results. An edit to the principle is not necessary to capture the intent of software independence.
6/7/23	Citizens' Oversight Projects - Ray Lutz	2.0	9.1.1-A	The voting system must be software independent. 1. ~~The voting system must meet the requirements within the Paper-based System Architectures or Cryptographic E2E Verifiable System Architectures section, or both.~~ ... The~~re are currently two~~ method~~s~~ specified in the VVSG for achieving software independence: • through the use of independent voter-verifiable paper records, and • ~~cryptographic E2E verifiable voting systems.~~ Paper-based ~~and cryptographic E2E verifiable~~ system architectures ~~are~~ may be software independent ~~and both can be used within the same voting system. In this case where a voting system is identified as being a combination of both architectures, the system would need to be compliant with both sets of requirements. However, a system that meets all of the paper-based requirements need not satisfy the E2E-requirements even if it incorporates E2E-verifiable functionality.~~ COMMENT: no software independent E2E Verifiable systems have been approved nor adequately demonstrated, and are only considered software independent if they actually are. Deeming them software independent up front does not mean they actually will be so.		Requires further investigation	Discussion with other stakeholder concerning E2E required	Partial Accept, Discussion	I agree with the "may be" edit. Paper-based systems also have to prove that they are software independent. I believe the VVPAT paper roll systems are examples of systems that were not necessarily software independent. Or a system that does not include a full reading of the ballot selections (e.g., only a barcode) would not be software independent.
8/2/22	Government Blockchain Association	2.0	9.1.1-A – Software independent The voting system must be software independent. 1. The voting system must meet the requirements within the Paper-based System Architectures or Cryptographic E2E Verifiable System Architectures section, or both. 2. The voting system documentation must include the method used to provide software independence.	The following test assertion associated with this requirement needs to be modified. To be considered for modification. More discussion needed. TA911A-1-2: IF a voting system is an E2E system THEN it MUST produce cryptographic proof of the validity of cast votes as defined in section 9.1.6.		Reject	Out of scope. Remote Delivery, mark and return is outside of Voting Systems.	Agree with EAC decision	Out of scope

Attachment 1 - 2023 Proposed VVSG Changes

Date	Organization	VVSG	Requirement	Proposed Changes / Additions *Note that red indicates an addition to an existing requirement, and strikethrough indicates removal from an existing requirement.*	Comment / Reasoning	EAC Initial Decision	EAC comment	NIST Initial Decision	NIST Comment
6/21/23	Smartmatic	2.0	General	New CDF standards are being published by NIST. Is there a policy around their inclusion in VVSG?	Recommend establishing an effectivity policy for new CDF's.	Accepted	Only CDFs in the VVSG are required. New CDF publications will need to be added to a future VVSG revision in order to be required.	Agree with EAC decision	
6/7/23	Citizens' Oversight Projects - Ray Lutz	2.0	9.1.2-A	Discussion Tamper-evident records include CVRs, ballot images ~~and artifacts from a cryptographic E2E verifiable voting system~~. The record also ensures that identified issues and other problems cannot be lost or unintentionally modified once they are discovered		Requires further investigation	Discussion with other stakeholder concerning E2E required	Reject	NIST recommends keeping all requirements or any information related to E2EV Systems to support innovation and future E2EV systems. Inclusion of the E2EV requirements helps prevent any potential delays in the process or progress towards E2EV systems.
5/20/23	State Audit Working Group (SAWG)	2.0	9.1.2-B	9.1.2-B – Tamper-evident record creation Paper records or other tamper-evident electronic records of the voter's ballot selections must be captured when each ballot is cast. Any ballot images from a scanner of hand- marked paper ballots or BMD-printed ballots must secure the images as soon as possible using hash values and trusted cryptographic signatures of groups of hash values to allow for detection of any future changes of those images and enable audits of the chain of custody of the paper ballots. The voting system must be able to show any selected ballot images from a batch, for checking immediately after scanning a batch.	Cryptographic signatures of images may be time stamped if that will not reveal the time or order of voting. It's important to enable quality control audits of image accuracy immediately after images are created and hashed, by selecting a random sample and comparing images to paper ballots.	Reject	Capability to generate ballot images needs to be supported but they are not necessarily required.	Agree with EAC decision	I believe this comment is covered in 13.2-A and B
5/20/23	State Audit Working Group (SAWG)	2.0	9.1.3-A	The voting system must provide individual voters the opportunity to verify that the ballot, whether a hand-marked paper ballot or a BMD-printed ballot, reflects their selections before casting it. ~~that the voting system correctly interpreted their ballot selections.~~	It is the ballot that the voter must be able to verify, not how the voting system interpreted that ballot. Generally, scanners do not allow the voter to verify how the ballot was interpreted. Showing the voter the interpretation would be a huge change and could affect privacy and throughput.	Reject	Scanners and other devices where the voter marks and casts a paper ballot are required to provide a full ballot selection review screen. As per requirement 7.3-G.	Agree with EAC decision	A component of the voting system is used to verify the interpetation of the ballot. Hand-marked paper ballots are not a technical piece of equipment used to verify selections.
6/7/23	Verified Voting	2.0	9.1.3-A	The requirement that voters be able to verify that the voting system correctly "interpreted" their ballot selections is inscrutable. We believe the intention is that voters be able to verify that their ballot selections are correctly "recorded," either on a voter verified paper record or in an end-to-end verifiable digital record.		Reject	Scanners and other devices where the voter marks and casts a paper ballot are required to provide a full ballot selection review screen. As per requirement 7.3-G.	Partial Accept, See suggested edits.	"correctly recorded" implies that there is verification that ballot selections were correctly captured in the election results. This requires auditing. It may be reasonable to update the requirement to the following: *The voting system must provide individual voters the opportunity to verify how the voting system ~~correctly~~ interpreted their ballot selections.*
6/7/23	Citizens' Oversight Projects - Ray Lutz	2.0	9.1.3-A	Discussion • Voter-facing scanners and other vote-capture devices can be used to meet this requirement. An electronic ballot marker can print a voter's ballot selections to review before casting. ~~An E2E verifiable system can print a receipt that allows a voter to verify their selections are tabulated and captured correctly~~. Principle 7: Marked, Verified, and Cast as Intended includes more requirements for voter verification.		Requires further investigation	Discussion with other stakeholder concerning E2E required	Reject	NIST recommends keeping all requirements or any information related to E2EV Systems to support innovation and future E2EV systems. Inclusion of the E2EV requirements helps prevent any potential delays in the process or progress towards E2EV systems.
8/2/22	Government Blockchain Association	2.0	9.1.4-A – Auditor verification Voting systems must generate records that would enable external auditors to verify that cast ballots were correctly tabulated.	The following test assertion associated with this requirement needs to be modified. TA914A-1: IF an external auditor is given voting system records, THEN the auditor MUST be able to validate that all cast ballots were correctly tabulated.		Reject	Out of scope. Remote Delivery, mark and return is outside of Voting Systems.	agree with EAC decision	

Attachment 1 - 2023 Proposed VVSG Changes

Date	Organization	VVSG	Requirement	Proposed Changes / Additions *Note that red indicates an addition to an existing requirement, and strikethrough indicates removal from an existing requirement.*	Comment / Reasoning	EAC Initial Decision	EAC comment	NIST Initial Decision	NIST Comment
6/21/23	Smartmatic	2.0	General	New CDF standards are being published by NIST. Is there a policy around their inclusion in VVSG?	Recommend establishing an effectivity policy for new CDF's.	Accepted	Only CDFs in the VVSG are required. New CDF publications will need to be added to a future VVSG revision in order to be required.	Agree with EAC decision	
5/20/23	State Audit Working Group (SAWG)	2.0	9.1.5-C	The recorded ballot selections must be presented in a human-readable format that is understandable by the voter. The voting system must be evaluated for usability by voters both in terms of the rate at which voters thoroughly review their ballots and in terms of how successful they are in discovering any discrepancies between the ballot and their intended selections. Discussion The requirement ensures that a human-readable version of the data is also printed whenever a barcode is used to encode ballot selections. The intelligibility of the paper record affects both the rate at which voters review their ballots and the rate at which voters discover any discrepancies between the ballot and their intended selections.	See suggested 7.3-II. A voting system with an electronic interface must inform the voter that the paper hand-marked or BMD-printed ballot is the official record of their vote and that the voter should check the ballot before casting it.	Reject	This is accuracy testing, and this required for 'all paper based architectures'.	Agree with EAC decision	The requirements are not the right place to discuss successful ballot review and the rate at which voters review.
9/21/22	NIST	2.0	9.1.5-D – Matching selections All representations of a voter's ballot selections produced by the voting system must **agree with** the selections made by the voter.	Is "agree" plain language? Suggestion to substitute "match" for "agree with".		Accepted	Changed in errata	Agree with EAC decision	NIST Submitted comment
6/7/23	Free Speech for People	2.0	9.1.5-F	Recommended addition at the end:"…not seen by the voter or anyone in the presence of the voter." The unique ballot identifier generated to facilitate audits should not be known to the voter, or anyone.	Black and blue are the most common colors used by voters. If machines use other colors, it will usually be possible to distinguish between voter & machine marks on original paper ballots, even when machines malfunction and drip ink unexpectedly.	Requires Further Investigation	To be investigated This is also being subject to an RFI with CBG.	Reject	The unique identifier can be known by the voter because it does not prove that the ballot belongs to the voter and does not show how a voter voted. We did not specifiy where the unique identifier should be located. Ideally, this should not be a secret modifcation to the ballot.
5/20/23	State Audit Working Group (SAWG)	2.0	9.1.5-G	"Instead the voting system should only be physically able to print outside of the bounds of the ballot selection" in Comments		Reject	Incorporate TA into requirement	Agree with EAC decision	
6/7/23	ADT		9.1.5-G	We suggest clarifying that the system should be not merely disabled from printing on the ballot selection area via software, but physically unable to print over the ballot selection area. Discussion After a voter verifies and submits their ballot, a voting system may print on paper ballot to apply a unique identifier that is later used for auditing purposes. To preserve software independence the voting system should not be physically able to print over or within the ballot selection area because that would cause an undetectable change to the election outcome. Instead the voting system should only be physically able to print outside of the bounds of the ballot selection area and may also create further distinction by printing in a different font style or color		Reject	Recommended change does not met the intent of the requirement.	Agree with EAC decision	The discussion could imply a software and/or a physical disabling of printing in the ballot selection area to ensure software independence is preserved.

Attachment 1 - 2023 Proposed VVSG Changes

Date	Organization	VVSG	Requirement	Proposed Changes / Additions *Note that red indicates an addition to an existing requirement, and strikethrough indicates removal from an existing requirement.*	Comment / Reasoning	EAC Initial Decision	EAC comment	NIST Initial Decision	NIST Comment
6/21/23	Smartmatic	2.0	General	New CDF standards are being published by NIST. Is there a policy around their inclusion in VVSG?	Recommend establishing an effectivity policy for new CDF's.	Accepted	Only CDFs in the VVSG are required. New CDF publications will need to be added to a future VVSG revision in order to be required.	Agree with EAC decision	
6/7/23	Citizens' Oversight Projects - Ray Lutz	2.0	9.1.6	Entire guideline should be moved to an appendix		Requires Further Investigation	Discussion with other stakeholder concerning E2E required	Reject	9.1.6 is not a guideline. NIST recommends keeping all requirements related to E2EV Systems to support innovation and future E2EV systems. Inclusion of the E2EV requirements helps prevent any potential delays in the process or progress towards E2EV systems.
6/7/23	Citizens' Oversight Projects - Ray Lutz	2.0	9.1.6.-E	COMMENT: Receipts are a very difficult component to add and inevitably can provide a potential for linking the voter to their ballot, particularly by election administrators. This is not true of paper-based systems once the paper has been merged with the other paper ballots and sufficiently anonymized. However, even without E2E verifiability, such receipts could be provided in the proposed ballot-image based system. We gain significant advantages using traditional cybersecurity measures without mandating the very difficult requirement of receipts.		Requires Further Investigation	Discussion with other stakeholder concerning E2E required	No action required	NIST recommends keeping all requirements related to E2EV Systems to support innovation and future E2EV systems. Inclusion of the E2EV requirements helps prevent any potential delays in the process or progress towards E2EV systems.
6/7/23	Citizens' Oversight Projects - Ray Lutz	2.0	9.1.6-C	COMMENT: The systems as proposed do not provide evidence of this type because the voter cannot look at their ballot choices as recorded by the device, but only an indirect representation. Therefore, this has not been demonstrated by the systems usually described as potential E2E systems.		Requires Further Investigation	Discussion with other stakeholder concerning E2E required	No action required	NIST recommends keeping all requirements or any information related to E2EV Systems to support innovation and future E2EV systems. Inclusion of the E2EV requirements helps prevent any potential delays in the process or progress towards E2EV systems.
6/7/23	Citizens' Oversight Projects - Ray Lutz	2.0	9.1.6-F	COMMENT: Ballot Receipts may result in significant misinformation campaigns that maybe technically possible to clear up using mathematical proofs, but may never be feasible to convince the general public.		Requires Further Investigation	Discussion with other stakeholder concerning E2E required	No action required	NIST recommends keeping all requirements related to E2EV Systems to support innovation and future E2EV systems. Inclusion of the E2EV requirements helps prevent any potential delays in the process or progress towards E2EV systems.
6/7/23	Citizens' Oversight Projects - Ray Lutz	2.0	9.1.6-G	COMMENT: "Evidence" as used here are cryptographic hashes which will provide the general public with no warm fuzzy feeling that the election was conducted properly, just the opposite.		Requires Further Investigation	Discussion with other stakeholder concerning E2E required	No action required	NIST recommends keeping all requirements or any information related to E2EV Systems to support innovation and future E2EV systems. Inclusion of the E2EV requirements helps prevent any potential delays in the process or progress towards E2EV systems.

Attachment 1 - 2023 Proposed VVSG Changes

Date	Organization	VVSG	Requirement	Proposed Changes / Additions *Note that red indicates an addition to an existing requirement, and strikethrough indicates removal from an existing requirement.*	Comment / Reasoning	EAC Initial Decision	EAC comment	NIST Initial Decision	NIST Comment
6/21/23	Smartmatic	2.0	General	New CDF standards are being published by NIST. Is there a policy around their inclusion in VVSG?	Recommend establishing an effectivity policy for new CDF's.	Accepted	Only CDFs in the VVSG are required. New CDF publications will need to be added to a future VVSG revision in order to be required.	Agree with EAC decision	
6/7/23	Citizens' Oversight Projects - Ray Lutz	2.0	9.1.6-H	COMMENT: "encoded ballots" cannot provide any assurance to the general public because they are not human-readable.		Requires Further Investigation	Discussion with other stakeholder concerning E2E required	No action required	NIST recommends keeping all requirements or any information related to E2EV Systems to support innovation and future E2EV systems. Inclusion of the E2EV requirements helps prevent any potential delays in the process or progress towards E2EV systems.
6/7/23	Citizens' Oversight Projects - Ray Lutz	2.0	9.1.6-I	COMMENT: A "bulletin board" is an insufficient method for posting election evidence. And if the evidence is so heavily obscured that the public can't recognize them as "ballots "then this will never be acceptable to the general public.		Requires Further Investigation	Discussion with other stakeholder concerning E2E required	No action required	NIST recommends keeping all requirements related to E2EV Systems to support innovation and future E2EV systems. Inclusion of the E2EV requirements helps prevent any potential delays in the process or progress towards E2EV systems.
6/7/23	Florida Fair Elections Coalition	2.0	9.2.	VVSG Section 9.2-A – Audit support documentation, states that "Ballots, CVRs, and ballot images are examples of artifacts that can support a post-election audit." Again, these records cannot support a post-election audit if they have not been retained. All voting systems should be set up to only allow the retention of ALL ballot images		Reject	It is not a requirement to retain images of ALL ballot images.	Reject.	The discussion mentions ballot images as an option.
6/7/23	Chris Sautter	2.0	9.2-A and 13.1-A	I respectfully request that language be added to 13.1(2) Data Protection of Election records and 9.2-A Audit Support Documentation to require that voting systems not be allowed to delete ballot images. The practice of permitting ballot images to be deleted by programming voting machines to save only write-in ballot images or no ballot images is clearly in violation of federal law. (52 USC 20701). The U.S. Department of Justice issued a July 29, 2021 directive stating: The materials covered by Section 301 extend beyond 'papers' to include other 'records.' Jurisdictions must therefore retain and preserve records created in digital or electronic form such as ballot images.		Requires Further Investigation	It is not a requirement to retain images of ALL ballot images. The ability to remove/delete ballot images is a function that must be available to met state statutes	Reject	Agreed. The ability to remove CVRs and ballot images is necessary and is restricted to admins who use MFA and must be logged.
5/20/23	State Audit Working Group (SAWG)	2.0	9.3-B	9.3-B – Chain-of-custody support for a voting system Images (and any associated hashes and digital signatures) are available to help protect the chain of custody of the paper ballots and of the images themselves.		Reject	Already covered in other requirements. Recommended language is not a requirement format.	Agree with EAC decision	covered through integrity protection requirements
5/20/23	State Audit Working Group (SAWG)	2.0	9.4-A	in Comments "An evidence-based election requires convenient access to ballot sheets, ballot sheet images, and cast vote records, and hashes or digital signatures of images and CVRs for efficient and trustworthy public tabulation audits. Vendors should demonstrate how an election system provides all the information necessary for an independent Risk-Limiting Audit (RLA) (both single ballot-level comparison audits and batch comparison audits)."		Reject	RLA requires either unique identifier or to be scanned in order (for Central Count)	Agree with EAC decision	Some of suggested edits are covered through other requirements

Attachment 1 - 2023 Proposed VVSG Changes

Date	Organization	VVSG	Requirement	Proposed Changes / Additions *Note that red indicates an addition to an existing requirement, and strikethrough indicates removal from an existing requirement.*	Comment / Reasoning	EAC Initial Decision	EAC comment	NIST Initial Decision	NIST Comment
6/21/23	Smartmatic	2.0	General	New CDF standards are being published by NIST. Is there a policy around their inclusion in VVSG?	Recommend establishing an effectivity policy for new CDF's.	Accepted	Only CDFs in the VVSG are required. New CDF publications will need to be added to a future VVSG revision in order to be required.	Agree with EAC decision	
6/7/23	Verified Voting	2.0	9.4-A	This discussion is welcome but would benefit from further refinement. 9.4-A states, "A paper-based voting system must produce paper records that allow election officials to conduct a risk-limiting audit." It is unclear what paper records are intended here beyond the voter-verifiable paper records discussed under 9.1.5, Paper records. As the discussion of 9.4-A makes clear, some digital records-at bare minimum, ballot manifests-typically are integral to risk-limiting audits. The language of 9.1.4-A, Auditor verification, appropriately is more general: "Voting systems must generate records that would enable external auditors to verify that cast ballots were correctly tabulated." We suggest removing the word "paper" from 9.4-A in parallel: "A paper-based voting system must produce records that allow election officials to conduct a risk-limiting audit." Additional changes may be helpful.		Requires Further Investigation	Second recommendation may be considered for removing the word "paper" and allow for more than just paper records to be considered, collected, and used in RLAs.	Accept	**Update requirement:** A paper-based voting system must produce ~~paper~~ records that allow election officials to conduct a risk-limiting audit.
5/20/23	State Audit Working Group (SAWG)	2.0	9.4-B	Voting systems that generate or rely on random or pseudo-random numbers for auditing purposes must document the method used to obtain the numbers, how the sequence of random numbers cannot be associated with the order in which ballot sheets were read, and how the random numbers are used within the voting system.		Requires Further Investigation	RNGs fall into cryptographic modules which require FIPs. Further investigation with NIST.	Accept	The suggested change adds clarification to what can be included in the documentation.
5/20/23	State Audit Working Group (SAWG)	2.0	9.4-C	The voting system must enable election auditors to easily and uniquely address individual ballot sheets using a unique identifier. Such ballot identifiers must not allow the voter to be matched up to the ballot, ballot image, or cast vote record.		Reject	"Easily" is undefined, and ambiguous. Other changes are addressed in other requirements	Partial Accept, See suggested edits.	Consider adding related requirements: 10.2.2-E, 9.1.5-F, 9.4-B
6/7/23	Verified Voting	2.0	9.4-C	This important requirement should be clarified. For paper-based voting systems, auditability typically entails that election auditors must be able to address individual voter verified paper records, or ballot sheets. The ballot sheets of multi-page ballots (referenced without discussion in 9.4-D) often cannot be reliably associated after ballots are cast, and may even be deliberately separated to protect ballot secrecy. Adding the phrase "or ballot sheets" as follows may suffice to generalize the requirement to both paper-based and end-to-end verifiable systems: "The voting system must enable election auditors to uniquely address individual ballots or ballot sheets." The discussion of 9.4-C notes that "The unique ballot identifier must not tie a ballot to an individual voter." However, the corresponding test assertion does not address this requirement. This omission is significant because unique ballot identifiers assigned by voter-facing scanners-unlike identifiers assigned by batch-fed scanners-must be randomized to obfuscate the order in which ballots were cast. Unfortunately, not all implementations of pseudo-random numbers obfuscate the order. We recommend adding a test assertion to ensure that voter-facing scanners that imprint non-serialized unique ballot identifiers do so in a manner that satisfies the requirement and also meets the standard specified under 10.2.2-E - Randomly generated identifiers. Also, the discussion of 9.4-C should clarify that this requirement is needed to support ballot-level comparison RLAs, not all RLAs as follows [new text italicized]: "This capability is needed to support ballot-level comparison RLAs."	Note that there is a long discussion in the original submission They are recommending the additional language to ensure that ballot identification cannot be associated with voters or tracked by time stamps giving someone the ability to associate voter and ballot.	Accept first part of this comment. The remainder should be investigated further.	"or ballot sheets" should be sufficient.	*Agree that this needs further research.*	If we add "ballot sheets", do we need to add a definition to the glossary? We also use the term "ballot sheet" in 9.4.A.

Attachment 1 - 2023 Proposed VVSG Changes

Date	Organization	VVSG	Requirement	Proposed Changes / Additions *Note that red indicates an addition to an existing requirement, and strikethrough indicates removal from an existing requirement.*	Comment / Reasoning	EAC Initial Decision	EAC comment	NIST Initial Decision	NIST Comment
6/21/23	Smartmatic	2.0	General	New CDF standards are being published by NIST. Is there a policy around their inclusion in VVSG?	Recommend establishing an effectivity policy for new CDF's.	Accepted	Only CDFs in the VVSG are required. New CDF publications will need to be added to a future VVSG revision in order to be required.	Agree with EAC decision	
6/7/23	Verified Voting	2.0	9.4-E	1. The ability to export batch subtotals in a machine-readable format should at least be listed among the "example features/paper records" in the discussion. We recommend that it be formally required and tested for. 1.1.5-G, Record audit information, already requires CVRs to include "identification of the batch containing the corresponding voted ballot, when applicable"-information that supports voting system export of ballot manifests (although any such manifests should be checked in compliance audits) and also can support batch subtotals. For instance, the following could be added as 9.4-E -Batch reporting: "The voting system must be able to export batch subtotals [compliant with CDF specifications]."		Require further investigation.	It is allowed, and possibly a good practice. Does it need to be made required? Clarification on reports including results information. Batch information is allowed, Early result reporting cannot be a federal requirement.	Partial Accept, Discussion	I believe this is referring to 9.4-A. It could be reasonable to include mention in the discussion. **An edit to 1.1.9-B may address the concern** - "The voting system must have the capability to create post-election reports that contain cast ballot counts and vote counts for contests on the ballot types served by precincts or splits of precinct; When the voting system supports batching, it must have the capability to create these reports by batch."
8/2/22	Government Blockchain Association	2.0	Principle 10 Ballot Secrecy	New requirement needs to be added to accommodate remote digital ballot delivery, marking, and return. GBA-WG-14 The system shall not be able to count ballots earlier than a moment in time specified by the jurisdiction.		Reject	Out of scope. Remote Delivery, mark and return is outside of Voting Systems.	Agree with EAC decision	out of scope
8/2/22	Government Blockchain Association	2.0	Principle 10 Ballot Secrecy	New requirement needs to be added to accommodate remote digital ballot delivery, marking, and return. GBA-WG-12 The immutable record shall be available in a human readable format at the appointed time.		Reject	Out of scope. Remote Delivery, mark and return is outside of Voting Systems.	Agree with EAC decision	Out of scope
6/7/23	Verified Voting	2.0	10.1-A	The discussion notes, in the context of ballot secrecy, that "the voting system cannot prevent a voter from self-identifying within write-in fields or other areas of the ballots." We suggest noting that this concern extends to unredacted ballot images and, potentially, CVRs. These digital artifacts can pose additional threats to ballot secrecy. (The requirements for guideline 10.2 grapple with this conundrum.) We do not believe VVSG 2.0 can be expected to resolve the policy questions pertaining to ballot images and CVRs. Nevertheless, some reference to the underlying ballot secrecy concerns would provide helpful context.		Noted		Agree with EAC decision	
5/20/23	State Audit Working Group (SAWG)	2.0	10.2.1-B	10.2.1-B – Indirect voter associations No systems may use indirect voter association. ~~Indirect voter associations must only be used to associate a voter with their encrypted ballot selections.~~ Comments Indirect voter associations jeopardize ballot secrecy. Eligibility mismatches must be determined prior to including ballots in the tabulation. Votes legitimately cast by a voter during the allowable voting period should not be able to be retrieved even if the voter dies; the danger to the integrity of an election by degrading ballot secrecy far outweighs any questionable and small advantage. Signature mismatches and death of voters do not specifically relate to Cryptographic E2E systems. ~~This requirement only applies to paperless voting systems that also meet the requirements under Guideline 9.1, which states that the voting system must be software independent. During the writing of these requirements, cryptographic E2E verifiable voting systems are a potential paperless and software independent system that could be applicable for this requirement.~~		Requires further investigation	Discussion with other stakeholder concerning E2E required	Reject	NIST recommends keeping all requirements related to E2EV Systems to support innovation and future E2EV systems. Inclusion of the E2EV requirements helps prevent any potential delays in the process or progress towards E2EV systems.

Attachment 1 - 2023 Proposed VVSG Changes

Date	Organization	VVSG	Requirement	Proposed Changes / Additions *Note that red indicates an addition to an existing requirement, and strikethrough indicates removal from an existing requirement.*	Comment / Reasoning	EAC Initial Decision	EAC comment	NIST Initial Decision	NIST Comment
6/21/23	Smartmatic	2.0	General	New CDF standards are being published by NIST. Is there a policy around their inclusion in VVSG?	Recommend establishing an effectivity policy for new CDF's.	Accepted	Only CDFs in the VVSG are required. New CDF publications will need to be added to a future VVSG revision in order to be required.	Agree with EAC decision	
6/7/23	Citizens' Oversight Projects - Ray Lutz	2.0	10.2.1-B, C,D,E,F	Delete Entirely		Requires further investigation	Discussion with other stakeholder concerning E2E required	Reject	NIST recommends keeping all requirements related to E2EV Systems to support innovation and future E2EV systems. Inclusion of the E2EV requirements helps prevent any potential delays in the process or progress towards E2EV systems.
5/20/23	State Audit Working Group (SAWG)	2.0	10.2.1-C	10.2.1-C Recallable Ballots Ballots may never be recallable. Discussion A recallable capability alone could reduce the confidence of voters and be used by some to spread distrust of voting systems. It also could open up the voting system to insider attack and vote buying and selling schemes. There is never a need to have an electronic provisional ballot. A hand-marked provisional paper ballot or BMD-printed provisional ballot can be used in a voter-facing system. ~~Use of indirect voter associations The voting system must only use indirect voter associations when the option is selected at the beginning of a voting session for situations when a voter needs to fill out a ballot before their eligibility is determined.~~	The desire of a tiny number of jurisdictions which wish to require recallable ballots should not be used to allow highly dangerous capabilities in the voting machines used by the rest of the country.	Requires further investigation	Discussion with other stakeholder concerning E2E required	Reject	The suggested requirement is only applicable for paper-based systems and is not allowed through current requirements.
5/20/23	State Audit Working Group (SAWG)	2.0	10.2.1-D, 10.2.1 E-F	Remove entirely.	There is never a need for an electronic provisional ballot. A hand marked paper ballot or BMD-printed ballot can be used in a voter-facing system.	Requires further investigation	Discussion with other stakeholder concerning E2E required	Reject	NIST recommends keeping all requirements related to E2EV Systems to support innovation and future E2EV systems. Inclusion of the E2EV requirements helps prevent any potential delays in the process or progress towards E2EV systems.
5/20/23	State Audit Working Group (SAWG)	2.0	10.2.2.-B	A voter-facing voting system must not collect or contain data or metadata ~~associated with the~~ such as data in CVR and ballot image files that can be used to determine the order in which ~~ballots votes are cast~~ voters cast ballots.		Reject	Requirement applies to all components of voting systems, not only voter facing ones. Last strikethrough corrected in errata.	agree with EAC decision	
6/7/23	ADT		10.2.2.-F	All methods of voting supported by a voting system must produce voted ballots of similar size, shape, and layout; or the manufacturer must provide procedures to be used to ensure that sufficient numbers of ballots of each type are cast to ensure ballots cannot be easily associated with individual voters on the basis of ballot type.		Reject	Jurisdictions have implemented different procedures for this, and the definition of 'sufficient; varies amongst them.	Agree with EAC decision	This is more about process. VVSG 2.0 pg. 11 discusses this concern.
6/7/23	Citizens' Oversight Projects - Ray Lutz	2.0	10.2.2-A	Delete Entirely		Requires further investigation	Discussion with other stakeholder concerning E2E required	Reject	NIST recommends keeping all requirements related to E2EV Systems to support innovation and future E2EV systems. Inclusion of the E2EV requirements helps prevent any potential delays in the process or progress towards E2EV systems.

Attachment 1 - 2023 Proposed VVSG Changes

Date	Organization	VVSG	Requirement	Proposed Changes / Additions *Note that red indicates an addition to an existing requirement, and strikethrough indicates removal from an existing requirement.*	Comment / Reasoning	EAC Initial Decision	EAC comment	NIST Initial Decision	NIST Comment
6/21/23	Smartmatic	2.0	General	New CDF standards are being published by NIST. Is there a policy around their inclusion in VVSG?	Recommend establishing an effectivity policy for new CDF's.	Accepted	Only CDFs in the VVSG are required. New CDF publications will need to be added to a future VVSG revision in order to be required.	Agree with EAC decision	
6/7/23	Verified Voting	2.0	10.2.2-B	The discussion states: "No data or metadata is allowed whether in CVRs and ballot images or elsewhere if that metadata can be used to associate a voter with a record of voter intent. For instance, date of creation of record in the voter-facing device might reveal the order of voting. It is unclear whether the discussion intends to forbid including creation date in CVRs and other artifacts, or only to take whatever precautions are needed to avoid revealing voter record order. (See our discussion above under point 3 of 9.4-A.) We would prefer the latter approach, which could be supported by adding to the current language: "...might reveal the order of voting unless steps are taken to prevent this." Including creation dates in most early voting CVRs, combining dates if necessary to protect ballot privacy, appears to be the simplest and best way of allowing early voting ballots to be audited in smaller batches.		Requires further investigation	Date / time not specifically disallowed. NIST glossary of Metadata does include date / time.	Partial Accept, See suggested edits.	**Update Requirement Title and Text:** 10.2.2-B – No voter intent ~~record order~~ information The voting system must not contain data or metadata associated with the CVR and ballot image files that can be used ~~to determine the order in which ballots votes are cast~~ to associate a voter with a record of voter intent.
6/7/23	Citizens' Oversight Projects - Ray Lutz	2.0	10.2.2-E	COMMENT: In the provision above, we support the use of a hardware Trusted Platform Module which can generate random numbers as the seed for use in number generators.		Noted		No action required	
5/20/23	State Audit Working Group (SAWG)	2.0	10.2.3-B	Discussion This ensures that any person, process, or other entity reading, writing, or performing other actions to the electronic audit trail is properly logged. This requirement applies ~~does not apply~~ when the CVR, ballot images, and ballot selections are stored on removable media and removed from the vote-capture device. Logging data allows detection if anyone is peeking at results before the election is closed.		Reject	This requirement is meant for EMS rather voting devices. Jurisdiction's laws determine access to election results.	Partial Accept, See suggested edits.	This applies to EMS and tabulators. Delete the last sentence in the discussion to avoid confusion.
6/7/23	Citizens' Oversight Projects - Ray Lutz	2.0	10.2.4-A	*Delete Entirely*		Requires further investigation	Discussion with other stakeholder concerning E2E required	Reject	NIST recommends keeping all requirements related to E2EV Systems to support innovation and future E2EV systems. Inclusion of the E2EV requirements helps prevent any potential delays in the process or progress towards E2EV systems.
5/20/23	State Audit Working Group (SAWG)	2.0	10.2.4-B	Discussion The voting system needs to be constructed so that the security of the system does not rely upon the secrecy of the event logs. It will be considered routine for event logs to be made available to election officials, and ~~possibly even~~ to the public, ~~if election officials so desire~~, if permitted by law. The system will be designed to permit the election officials to access event logs without fear of negative consequences to the security and integrity of the election. For example, cryptographic secret keys or passwords will not be logged in event log records.		Reject	Only permitted by law is already implied.	Agree with EAC decision	
5/20/23	State Audit Working Group (SAWG)	2.0	10.2.4-C	Ballot activation devices must not create or retain information that can be used to identify a voter's ballot, including the order and time at which a voter uses the voting system. The ballot activation device must not be able to transport voter selections from the BMD back to the e-pollbook.	Ballot Activation Device should be in the glossary.	Accept	Accept in principle, but would need to be re-written	Partial Accept, See suggested edits.	**Update Requirement:** The voting system must not create or retain information that can be used to identify a voter's ballot selections on a token used to activate the ballot. **Update Discussion:** Tokens used to activate a voter's ballot should not be able to violate ballot secrecy by being used to identify a voter's ballot selections.

Attachment 1 - 2023 Proposed VVSG Changes

Date	Organization	VVSG	Requirement	Proposed Changes / Additions *Note that red indicates an addition to an existing requirement, and strikethrough indicates removal from an existing requirement.*	Comment / Reasoning	EAC Initial Decision	EAC comment	NIST Initial Decision	NIST Comment
6/21/23	Smartmatic	2.0	General	New CDF standards are being published by NIST. Is there a policy around their inclusion in VVSG?	Recommend establishing an effectivity policy for new CDF's.	Accepted	Only CDFs in the VVSG are required. New CDF publications will need to be added to a future VVSG revision in order to be required.	Agree with EAC decision	
8/2/22	Government Blockchain Association	2.0	Principle 11 Access Control	New requirement needs to be added to accommodate remote digital ballot delivery, marking, and return. GBA-WG-15 The solution shall authenticate all users in accordance with one or more levels of the NIST SP-800-63-3 standards. Note: The authentication should be recorded on an immutable ledger.		Reject	Out of scope. Remote Delivery, mark and return is outside of Voting Systems.	Agree with EAC decision	Out of scope
8/2/22	Government Blockchain Association	2.0	Principle 11 Access Control	New requirement needs to be added to accommodate remote digital ballot delivery, marking, and return. GBA-WG-16 The system shall be resilient enough to ensure that the ballot is protected from a failure in the any component of the ballot delivery system.		Reject	Out of scope. Remote Delivery, mark and return is outside of Voting Systems.	Agree with EAC decision	Out of scope
5/20/23	State Audit Working Group (SAWG)	2.0	Principle 11 Access Control	Does ~~not~~ require role-based access control (RBAC)		Noted	Change made.	Reject	The VVSG does NOT require RBAC, but has requirements for when RBAC is used. This was highlighted because previous VVSGs required RBAC, but 2.0 does not.
6/21/23	Voting Works	2.0	11.1-D	Does this include while the system is in operation for voting? This seems a bit concerning. Seems like the goal would be that they are easily readable, easily accessible, and secure while the system is in operation. I can understand needing access if there is an anomaly or machine malfunction, but the way the requirement reads makes it sound like you could pop open a system during voting sessions and see/generate the logs. Maybe using a term other than "on demand," such as "upon request" or "The voting system must allow administrators to access logs quickly and easily, to allow for efficient monitoring, review, and issue resolution."		Requires further investigation	This seems similar to an RFI. Will require clarification.	Partial Accept, See suggested edits.	**Update Requirement:** "The voting system must allow ~~provide~~ administrators to access ~~to~~ logs ~~on demand, allowing~~ for ~~continuous monitoring and periodic review~~ monitoring, review, and issue resolution."
5/20/23	State Audit Working Group (SAWG)	2.0	11.3.1-D	11.3.1-D Multi-person authentication for particularly critical functions Critical functions should allow extra protection by enabling election offices to require two or more persons, presumably bi-partisan, to authenticate actions. Such protection would be similar to having two keys controlled by different people to open a safe.		Requires further investigation	This is an interesting proposition, requires investigation.	Reject.	There are multiple ways of addressing the insider threat such as detection monitoring an logging capabilities that are found within VVSG 2.0..
6/7/23	ADT		11.3.1-D	The voting system must be capable of using multi-person authentication for performing critical operations. (See 11.3.1-B – Multi-factor authentication for critical operations for examples of critical operations). Multi-person authentication capabilities enable election officials to choose to require (multi-factor) authentication from two or more users, presumably bipartisan, before executing actions.		Requires further investigation	An interesting proposition, requires investigation.	Reject	There are multiple ways of addressing the insider threat such as detection monitoring an logging capabilities that are found within VVSG 2.0..
9/21/22	NIST	2.0	12.1-B – Unauthorized physical access alert Voter-facing scanners and electronic BMDs must produce an alert if access to a restricted voting device component is detected during the activated voting stage.	Remove "during the activated voting stage". Include discussion notes on when the alert can be used “after powered on”. Update the discussion section for these requirements to state that “alerts provide real time notification of tampering” Or “Immediate alert of tampering”. ASSUMPTIONS: Is good to detect unauthorized physical access during any phase of elections in which system is running/operating/powered-on. Might need clarification of wording for that assumption.		Accept	Wording needs to be determined, but in principle we agree.	Agree with EAC decision	NIST Comment

Attachment 1 - 2023 Proposed VVSG Changes

Date	Organization	VVSG	Requirement	Proposed Changes / Additions *Note that red indicates an addition to an existing requirement, and strikethrough indicates removal from an existing requirement.*	Comment / Reasoning	EAC Initial Decision	EAC comment	NIST Initial Decision	NIST Comment
6/21/23	Smartmatic	2.0	General	New CDF standards are being published by NIST. Is there a policy around their inclusion in VVSG?	Recommend establishing an effectivity policy for new CDF's.	Accepted	Only CDFs in the VVSG are required. New CDF publications will need to be added to a future VVSG revision in order to be required.	Agree with EAC decision	
9/21/22	NIST	2.0	12.1-C – Disconnecting a physical device Voter-facing scanners and electronic BMDs must produce an alert if a connected component is physically disconnected during the activated voting stage.	Remove "during the activated voting stage". Include discussion notes on when the alert can be used “after powered on”. Update the discussion section for these requirements to state that “alerts provide real time notification of tampering” Or “Immediate alert of tampering”.		Accept	Wording needs to be determined, but in principle we agree.	Agree with EAC decision	NIST Comment
9/21/22	NIST	2.0	12.1-D – Logging of physical connections and disconnections The voting system must log when a voter-facing scanner, electronic BMD, or other component is connected or disconnected during the activated voting stage.	Remove "during the activated voting stage". Update discussion to include something about logging and access alerts need to be activated as early as possible in the boot process.		Accept	Wording needs to be determined, but in principle we agree.	Agree with EAC decision	NIST Comment
6/21/23	Smartmatic	2.0	12.2-D	As regards logically disabling ports by an Administrator, it seems that the intent of this clause is to prevent open ports as the overall lifecycle of the equipment progresses and as the lifecycle of an election progresses.	If so, then an addition to this clause that allows for an automated closing of unneeded ports, as defined by the lifecycle stages of an election and documented, would be a better control. If automated (and assuming the automation scheme passes evaluation) then Administrator control might not be needed.	Requires further investigation	An automated control, for example using a script, is not specifically banned.	Reject	The requirement does not need to be updated. This is not prohibited.
6/7/23	Florida Fair Elections Coalition	2.0	Principle 13	Election Systems & Software (ES&S) offers an option to election administrators to set up each election to “save all images, save write-in images only, or save no images.” This feature should not be allowed as part of any vendor’s voting system. Ballot images are an important audit record that should not be deleted/destroyed. Digital scanners create an image of the ballot and count the votes from the image, not from the paper ballot itself. The image is part of the chain-of-custody of every ballot and every vote. VVSG Principle 13, Data Protection, “requires digitally signed cast vote records and ballot images,” but these records cannot be digitally signed if the have not even been retained.		Noted	See previous responses for requiring all ballot images saved.	No action required	
5/20/23	State Audit Working Group (SAWG)	2.0	Principle 13	13.1 –The voting system prevents unauthorized access to or manipulation of configuration data, cast vote records, transmitted data, ~~or~~ audit records, or data associated with extended features.		Accepted	We agree in principle. EAC should investigate of rewording this.	Reject	Unclear how data associated with extended features is not included with configuration data.
5/20/23	State Audit Working Group (SAWG)	2.0	13.1.2-A	Integrity protection for election records The voting system must ~~integrity~~ either detect or prevent modification of CVRs and ballot images ~~when they are stored~~ anywhere within the voting system Discussion Applying access control can help prevent any unauthorized modifications to CVRs and ballot images. Applying integrity protection ensures that any unauthorized modifications to CVRs and ballot images can be detected. For example, ballot images can be integrity protected using a private key maintained in a Hardware Security Module and a cryptographic hash signature of the image collection along with a digital signature of a collection of hashes. The timing and content of the digital signature for the collection of hashes must ensure that votes cannot be linked to a voter.	Any CVRs and ballot images should be cryptographically hashed as soon as possible, and then secured using a digital signature of a collection of cryptographic hashes. The images should be exported in the same format that they were in when originally hashed, collected and signed, so hashes of the exported images match the earlier ones.	Accept first strikethrough, and reject the rest		Agree with EAC decision, See suggested edtis.	Only remove "integrity" from the requirement text

Attachment 1 - 2023 Proposed VVSG Changes

Date	Organization	VVSG	Requirement	Proposed Changes / Additions *Note that red indicates an addition to an existing requirement, and strikethrough indicates removal from an existing requirement.*	Comment / Reasoning	EAC Initial Decision	EAC comment	NIST Initial Decision	NIST Comment
6/21/23	Smartmatic	2.0	General	New CDF standards are being published by NIST. Is there a policy around their inclusion in VVSG?	Recommend establishing an effectivity policy for new CDF's.	Accepted	Only CDFs in the VVSG are required. New CDF publications will need to be added to a future VVSG revision in order to be required.	Agree with EAC decision	
5/20/23	State Audit Working Group (SAWG)	2.0	13.2 Guideline	Source and integrity of election records covers the requirement that CVRs and ballot images be digitally signed both when stored and before being transmitted. The EMS needs to be able to cryptographically certify all electronic voting records. Digital signatures of collections of hashes are a form of integrity protection that can also help trace the source of any updates or alterations to election records. The timing and content of the digital signature for the collection of hashes must ensure that votes cannot be linked to a voter		Reject		Agree with EAC decision	
5/20/23	State Audit Working Group (SAWG)	2.0	13.2-A	Cast vote records and ballot images must be cryptographically hashed ~~digitally~~ when created ~~stored~~ and, if modified during election processing, again cryptographically hashed before being transmitted or otherwise exported. Collections of hashes must be exported along with a digital signature for each collection. The timing and content of the digital signature for the collection of hashes must ensure that votes cannot be linked to a voter.		Reject	Cryptographic hashes do not sufficiently mitigate this threat, as election records could be altered and then re-hashed.	Agree with EAC decision	
6/7/23	Citizens' Oversight Projects - Ray Lutz	2.0	13.2-A	This section is insufficient. We agree that CVR and ballot images must be digitally signed. But more detail is required, including how those signatures can be expressed, verified by a third party, and provided to the public so they can be checked against the CVR and Ballot Image data. Cryptographic signatures are worthless if no one checks them.	FIPS 186-4 has been superseded with the publication of FIPS 186-5 (February 3, 2023). Per the Implementation Schedule clause (12) in FIPS 186-5, "To facilitate a transition to FIPS 186-5, FIPS 186-4 remains in effect for a period of one year following the publication of this standard, after which FIPS 186-4 will be withdrawn [on February 3, 2024]. During this period, agencies may elect to use cryptographic modules and practices that conform to this standard, or may elect to continue to use FIPS 186-4.	Reject	EAC to investigate FIPS 186-5	Agree with EAC decision, See suggested edtis.	Update reference to FIPS 186-5. Out of scope to go into detail about implementation.
5/20/23	State Audit Working Group (SAWG)	2.0	13.2-B	Add: 5. Not include information that provides order of voting for voter-facing systems.		Reject	This is already covered in 10.2.2-B, 10.2.2-D, 10.2.4-C	Agree with EAC decision	
6/7/23	Citizens' Oversight Projects - Ray Lutz	2.0	13.3.	Cryptographic algorithms deal with the requirements that cryptographic functionality be implemented in a cryptographic module validated against Federal Information Processing Standard (FIPS) 140 [NIST01]. ~~In addition, cryptographic functions specific to E2E cryptographic voting protocols must adhere to requirements set by the EAC and are omitted from FIPS 140-2 validation.~~ Devices using cryptography need to employ NIST approved algorithms, and the key used with Message Authentication Codes needs to have a specific security strength. Voting system documentation describes how key management is to be performed by election officials.		Requires further investigation	Requires discussion with E2E stakeholders	Reject	NIST recommends keeping all requirements and information related to E2EV Systems to support innovation and future E2EV systems. Inclusion of the E2EV requirements helps prevent any potential delays in the process or progress towards E2EV systems.
6/21/23	Voting Works	2.0	13.3-A	VVSG requires that cryptographic implementations should meet FIPS 140 requirements, but does not specify how meeting them is to be verified. EAC should promulgate a rule describing what verification criteria are, i.e. do the cryptographic implementations in systems have to be independently validated, or is the use of off-the-shelf cryptographic systems that have already been certified sufficient (e.g., OpenSSL)? Are the VSTLs required to do the verification in the former case, or can they contract it out to other entities?		Noted	RFI to Test Assertion or both.	Suggested Change	**Update Discussion:** Voting system manufacturers may integrate existing or commercially available cryptographic modules that have already been validated.

Attachment 1 - 2023 Proposed VVSG Changes

Date	Organization	VVSG	Requirement	Proposed Changes / Additions *Note that red indicates an addition to an existing requirement, and strikethrough indicates removal from an existing requirement.*	Comment / Reasoning	EAC Initial Decision	EAC comment	NIST Initial Decision	NIST Comment
6/21/23	Smartmatic	2.0	General	New CDF standards are being published by NIST. Is there a policy around their inclusion in VVSG?	Recommend establishing an effectivity policy for new CDF's.	Accepted	Only CDFs in the VVSG are required. New CDF publications will need to be added to a future VVSG revision in order to be required.	Agree with EAC decision	
6/7/23	Citizens' Oversight Projects - Ray Lutz	2.0	13.3-A	Cryptographic functionality must be implemented in a that meets current FIPS 140 validation, operating in FIPS mode. This applies to: ~~1. software cryptographic modules, and~~ 2. hardware cryptographic modules. Discussion Use of cryptographic modules validated at level 1 or above ensures that the cryptographic algorithms used are secure and correctly implemented. The current version of FIPS140[NIST01, NIST19a] and information about the NIST Cryptographic Module Validation Program are available under [NIST20e] in Appendix C: References. Note that a voting device can use more than one cryptographic module, ~~and quite commonly can use a software module for some functions and a hardware module for other functions.~~	COMMENT: To meet the expectations of the Executive Order, allowing software-based implementation of FIPS 104-2 should not be allowed. COMMENT: Making hardware security modules optional goes against improving cryptographic security and should be reversed per EO-14028. Please see our detailed description of≈	Reject	This does not seem meet the contents of the Executive Order.	Agree with EAC decision, See suggested edtis.	**Update discussion:**"... Note that a voting device can use more than one cryptographic module, ~~and quite commonly can use~~ such as a software module for some functions and a hardware module for other functions. "
3/6/23	EAC	2.0	13.3-A - Cryptographic module validation	Review language, especially "that meet current FIPS 140 validation". Define 'current', as opposed to 'historical' or 'retired' or similar. Also state 'current' as current at time of certification.		Accept	The language needs to be updated for next version.	Agree with EAC decision	
6/7/23	Citizens' Oversight Projects - Ray Lutz	2.0	13.3-B	Delete Entirely		Requires further investigation	Requires discussion with E2E stakeholders	Reject	NIST recommends keeping all requirements and information related to E2EV Systems to support innovation and future E2EV systems. Inclusion of the E2EV requirements helps prevent any potential delays in the process or progress towards E2EV systems.
6/7/23	Citizens' Oversight Projects - Ray Lutz	2.0	13.3-C	COMMENT: An example that fulfills the requirement for cryptographic strength with a security strength of at least 112-bits could be the Advanced Encryption Standard (AES) with a 128-bit key. The application employs NIST approved cryptographic algorithms to encrypt and decrypt data, ensuring a security strength that exceeds the minimum requirement of 112-bits. This level of cryptographic strength provides a high level of security against brute-force attacks and unauthorized access to the encrypted data.	PLEASE NOTE: This does not go far enough. We need to specify EXACTLY how all data is to be secured, not just provide boundaries.	Reject	EAC will not prescribe how to build voting systems.	Agree with EAC decision	
6/7/23	Citizens' Oversight Projects - Ray Lutz	2.0	13.3-D	COMMENT: The key used with Message Authentication Codes (MACs) is commonly referred to as the MAC key. In terms of security strength and tag length, a commonly used algorithm that meets the requirement of at least 112 bits security strength and a 96-bit tag length is the HMAC-SHA-256 algorithm. HMAC(Hash-based Message Authentication Code) is a widely used construction for creating MACs using cryptographic hash functions, and SHA-256 (Secure Hash Algorithm 256-bit) is a commonly used hash function. By using a 256-bit key with HMAC-SHA-256, the security strength requirement of at least 112 bits is satisfied. Additionally, the 96-bit tag length ensures a strong level of integrity and authenticity for the message being authenticated.		Noted		Agree with EAC decision	
6/7/23	Citizens' Oversight Projects - Ray Lutz	2.0	13.3-E	COMMENT: The VVSG should define this in a standard way rather than allowing each voting system to do it differently.		Reject	EAC will not prescribe how to build voting systems.	Agree with EAC decision	
6/7/23	Citizens' Oversight Projects - Ray Lutz	2.0	13.4-A	The VVSG should define Air-Gapped and mention here as the preferred method.		Reject	EAC will not prescribe how to build voting systems.	Agree with EAC decision	

Attachment 1 - 2023 Proposed VVSG Changes

Date	Organization	VVSG	Requirement	Proposed Changes / Additions *Note that red indicates an addition to an existing requirement, and strikethrough indicates removal from an existing requirement.*	Comment / Reasoning	EAC Initial Decision	EAC comment	NIST Initial Decision	NIST Comment
6/21/23	Smartmatic	2.0	General	New CDF standards are being published by NIST. Is there a policy around their inclusion in VVSG?	Recommend establishing an effectivity policy for new CDF's.	Accepted	Only CDFs in the VVSG are required. New CDF publications will need to be added to a future VVSG revision in order to be required.	Agree with EAC decision	
9/21/22	NIST	2.0	Principle 14 – System Integrity	May want to specifically require that the system be updatable and using the latest software. E.g., "Support Updates and Patches". ASSUMPTIONS: "Latest software" may be more nuanced. While a best practice in general, "latest software" is relative to tested baselines. Is covered elsewhere relative to recommendations surrounding appropriate configuration management plans and approved updates.		Accepted	We agree in principle. EAC should investigate of rewording this.	Reject	After additional consideration, a specific requirement may not be necessary and could be difficult to scope. Patches to address problems may be sufficiently covered under 14.2-J.
8/2/22	Government Blockchain Association	2.0	Principle 14 System Integrity	New requirement needs to be added to accommodate remote digital ballot delivery, marking, and return. GBA-WG-19 The system shall meet a minimum error rate in accordance with the VVSG accuracy requirement.		Reject	Out of scope. Remote Delivery, mark and return is outside of Voting Systems.	Agree with EAC decision	out of scope
6/7/23	Kevin Skoglund	2.0	14.2.	The voting system should not contain wireless communication devices, even if disabled.		Reject	Voting Systems may use internal networks to securely transfer data between devices and components, not using the internet. In addition COTS products often come with wireless capabilities that are disabled either logically or by physical removing of the modem.	Agree with EAC decision	Agree with EAC. Many COTs components/devices include wireless capabilities, but these can be disabled logically or physically to address the underlying security threats.
5/20/23	State Audit Working Group (SAWG)	2.0	14.2-C	Voting systems must ~~not~~ be disabled from ~~capable of~~ establishing wireless connections as provided in this section.	Wireless should not be allowed at all. Preventing wireless through software alone is not sufficient. There have been cases where a model without wireless capabilities was purchased and later updated to a model with wireless all through software changes. Wireless must be prevented by permanently disabling any wireless capability in the hardware. If wireless hardware were present, the system could be hacked to provide wireless access to data or to modify the voting system software.	Reject	Voting Systems may use internal networks to securely transfer data between devices and components, not using the internet. In addition COTS products often come with wireless capabilities that are disabled either logically or by physical removing of the modem.	Agree with EAC decision	Agree with EAC. Many COTs components/devices include wireless capabilities, but these can be disabled logically or physically to address the underlying security threats.
5/20/23	State Audit Working Group (SAWG)	2.0	14.2-D		Comment: If there is no wireless hardware, this indicator would be unnecessary.	Reject	Voting Systems may use internal networks to securely transfer data between devices and components, not using the internet. In addition COTS products often come with wireless capabilities that are disabled either logically or by physical removing of the modem.	Agree with EAC decision	Agree with EAC. Many COTs components/devices include wireless capabilities, but these can be disabled logically or physically to address the underlying security threats.
6/7/23	Free Speech for People	2.0	14.2-D, 14.2-E	We strongly urge the EAC to ensure the VVSG 2.0 reflects the provisions in the principles and guidelines as drafted by the TGDC, which prohibit voting systems from including the capability of connecting wirelessly to public networks. The VVSG 2.0 should either ban the inclusion of wireless networking devices in voting systems, or should require the wireless networking devices be physically disabled.		Reject	Voting Systems may use internal networks to securely transfer data between devices and components, not using the internet. In addition COTS products often come with wireless capabilities that are disabled either logically or by physical removing of the modem.	Agree with EAC decision	Agree with EAC. Many COTs components/devices include wireless capabilities, but these can be disabled logically or physically to address the underlying security threats.

Attachment 1 - 2023 Proposed VVSG Changes

Date	Organization	VVSG	Requirement	Proposed Changes / Additions *Note that red indicates an addition to an existing requirement, and strikethrough indicates removal from an existing requirement.*	Comment / Reasoning	EAC Initial Decision	EAC comment	NIST Initial Decision	NIST Comment
6/21/23	Smartmatic	2.0	General	New CDF standards are being published by NIST. Is there a policy around their inclusion in VVSG?	Recommend establishing an effectivity policy for new CDF's.	Accepted	Only CDFs in the VVSG are required. New CDF publications will need to be added to a future VVSG revision in order to be required.	Agree with EAC decision	
6/7/23	Alan Hassall (BlockCerts)	2.0	14.2-E	14.2-E External network restrictions is prohibiting the adoption of the latest, best technological practice – blockchain. 14.2-E – External network restrictions Except for a connection to a Proof of Authentication AI blockchain via its associated private wallet, a voting system must not be configured to: 1. establish a connection to an external network, or 2. connect to any device external to the voting system…		Reject	Voting Systems may use internal networks to securely transfer data between devices and components, not using the internet. In addition COTS products often come with wireless capabilities that are disabled either logically or by physical removing of the modem.	Agree with EAC decision	out of scope
12/13/21	SLI Compliance	2.0	14.2-E – External network restrictions A voting system must not be configured to: 1. establish a connection to an external network, or 2. connect to any device external to the voting system.C3G3E3:F3	SLI Compliance Inquiry: VVSG 2.0 doesn't permit devices or components from using external network connections. However there is no consideration given for Private connection types or cellular communications. Does this include: cellular connectivity, modem connectivity, VPLS (virtual Private Lan Service), Point to point leased lines, Virtual Leased Line (VLL), MPLS, SD-WAN? EAC Response: 14.2-E External Network Restrictions requirement is intended to restrict any use of an external network including external network equipment that would not be managed by the election office. In the examples given in the question, an ISP manages and updates the equipment (e.g., gateways, network nodes) and that equipment is not within the control of the election office. The external network equipment would also not likely be submitted for testing and certification. There may be a need to update the glossary to clearly define internal and external to be the following: i. "internal network" - networked devices that are procured and managed by an election office ii. "external network" - networking devices outside of the control of an election office that are managed and maintained by an Internet Service Provider (ISP).		Accept	Update to glossary to be made. Possibly reword.	Agree with EAC decision	This was previously discussed b/w NIST and EAC
6/7/23	Citizens' Oversight Projects - Ray Lutz	2.0	14.2-F	The above section should mention air-gapped as a mechanism to achieve security.		Reject	"Achieve security" is a very ambiguous term. Air gaps can assist in securing a voting system, but there are many other mechanists too. EAC will not prescribe how to build voting systems.	Agree with EAC decision	agree with eac decision
6/21/23	Smartmatic	2.0	14.2-K	While it is a good idea to have systems free of "well-known vulnerabilities" the manner in which this clause is written makes putting it into practice difficult. When combined with the associated Test Assertion, the idea of being free of "well known" (VVSG) and "listed" (Test Assertion) vulnerabilities is not feasible.	Recommend inclusion of a requirement that as part of the vulnerability management plan a Manufacturer must choose a criterion, such as CVSS score of 7 or higher for elimination of vulnerabilities. It would be important to note in such a criterion that many listed vulnerabilities arise when systems are connected to the Internet. These sorts of vulnerabilities should receive consideration and engineering judgement for elimination when applied in the context of VVSG, both assuming Internet connectivity is not occurring along with what would be the result if the voting system's closed/isolated network was indeed connected to the Internet. The Manufacturer's analysis of the system and its security posture must also be taken into account, but it is not in the current VVSG.	Requires further investigation	EAC will look at removing any ambiguity.		
5/22/23	Gisela Aaron AZ citizen	2.0	14.3 (Stated for the Lifecycle Policy, but would be belong in 14.3)	To promote voter trust and election integrity, all parts, chips and computer programs **shall** be **Made in USA**		Reject	Manufacturers have testified in Congress that 'chips' made in the US are not available .	Agree with EAC decision	

Attachment 1 - 2023 Proposed VVSG Changes

Date	Organization	VVSG	Requirement	Proposed Changes / Additions *Note that red indicates an addition to an existing requirement, and strikethrough indicates removal from an existing requirement.*	Comment / Reasoning	EAC Initial Decision	EAC comment	NIST Initial Decision	NIST Comment
6/21/23	Smartmatic	2.0	General	New CDF standards are being published by NIST. Is there a policy around their inclusion in VVSG?	Recommend establishing an effectivity policy for new CDF's.	Accepted	Only CDFs in the VVSG are required. New CDF publications will need to be added to a future VVSG revision in order to be required.	Agree with EAC decision	
6/21/23	Voting Works	2.0	14.3.1-A	This requirement does not specify the means by which cryptographic verification of the OS is to be performed. It also does not require a hardware root of trust, or verification of firmware or bootloader. This leaves a substantial gap in the security model, as malicious firmware or bootloaders could trivially circumvent verification steps by simply copying and presenting verification information from a known good OS, while booting a malicious OS. UEFI Secure Boot is one of the only known standards that solves these problems, and is widely supported on commodity devices due to Windows 11 requiring the presence and use of TPM 2.0 hardware coprocessors to verify firmware and bootloaders at system boot time.		Requires further investigation	EAC will look at this issue further.	Reject.	NIST recommends not going into specifics here.
6/7/23	Kevin Skoglund	2.0	14.3.1-A	"Cryptographic boot verification", states that "The voting system must cryptographically verify firmware and software integrity before the operating system is loaded into memory." However, as the Discussion section explains, it does not require a hardware root of trust or verification of the bootloader. This leaves a sizable security gap. If the bootloader were compromised, the subsequent cryptographic boot verification would be meaningless. It is my understanding that several voting system manufacturers have already implemented secure boot in some components, and I expect many will use it to satisfy Requirement 14.3.1-A. If this change is deemed larger than a minor change, then an alternative minor change would be to add text to the Discussion of 14.3.1-A reading, "Manufacturers are encouraged to establish a hardware root of trust and implement secure boot for future compatibility with anticipated VVSG requirements."	"Secure boot" is the term used when a hardware root of trust is used to verify that all software used to boot the computer is trustworthy. Since the development of VVSG 2.0, secure boot has become an industry standard. The majority of modern computers include a specialized chip which holds cryptographic data used to establish a hardware root of trust. The technology goes by many names, but the Trusted Platform Module (TPM) standard and Apple's T2 chip are the most common examples. This chip provides a trustworthy foundation for securing a variety of sensitive operations, including verification of the bootloader.	Requires further investigation	As previous comment - EAC will look at this issue further.	Suggested Change	**Update first sentence in discussion:** Hardware-based boot verification is encouraged but is not mandated by this requirement.
6/7/2023	Smartmatic	2.0	14.3-A, B, C	This set of Requirements should be re-written, brought together, and made into an integrated set of Supply Chain Management and Risk Management requirements.	With clarification regarding the Criticality Analysis, a consolidated Requirement could define minimum elements of a supply chain management program and incorporate risk management. As written in 2.0 the three Requirements are not well integrated; and the Discussion box under 14.3-C partially contradicts Requirements under Principle 3 (At minimum the bill of materials for critical components are required, but this does not restrict the voting system vendor from listing the bill of materials for other components.) which require a complete listing of all hardware and software used in the voting system.	Requires further investigation	EAC will look into this further.	Partial Accept, See suggested edits.	For 14.3-C, Add related requirements 3.1.1-C and include in discussion using the list from 3.1.1-C to identify the Critical Components.

Attachment 1 - 2023 Proposed VVSG Changes

Date	Organization	VVSG	Requirement	Proposed Changes / Additions *Note that red indicates an addition to an existing requirement, and strikethrough indicates removal from an existing requirement.*	Comment / Reasoning	EAC Initial Decision	EAC comment	NIST Initial Decision	NIST Comment
6/21/23	Smartmatic	2.0	General	New CDF standards are being published by NIST. Is there a policy around their inclusion in VVSG?	Recommend establishing an effectivity policy for new CDF's.	Accepted	Only CDFs in the VVSG are required. New CDF publications will need to be added to a future VVSG revision in order to be required.	Agree with EAC decision	
6/21/23	Smartmatic	2.0	14.3-B	criticality analysis - the new requirement has a good purpose; and during development the Manufacturer should determine critical components of their hardware and software so that they can initiate deeper treatment of those components and their supply chains. The two NIST publications cited provide little guidance to both setting up a criticality analysis program and to the actual analysis. They are too high level and abstract; and some of the material is not applicable to election equipment. Similarly, both the implied framework and the numerous restrictions on the analysis seen in the 14.3-B Discussion box and the associated Test Assertion should serve to indicate that this requirement needs additional analysis and clarification. Attempting to cut the fine lines between which software packages contribute to security, privacy, and [especially] performance and say which are critical, and at some high/medium/low level of criticality is not feasible, especially when the team takes the desired User Centered approach and considers effects on the voter. The logic behind any analysis process starts falling apart pretty quickly.	Recommend a review of this Requirement, its purpose, and consultation with persons who perform these analyses routinely in other industries to be able to cite (or author) more applicable references and guidance to Manufacturers.	Requires further investigation	As per previous comment. EAC will look into this further	Partial Accept, See suggested edits.	**Update requirment:** The voting system's documentation must include a list of critical components and suppliers defined by a criticality analysis and ~~supplier~~ impact analysis **Update Discussion due to NISTIR 8272 being withdrawn:** This can be supplemented by following NISTIR 8179 Criticality Analysis Process Model - Prioritizing Systems and Components [NIST18b] and ~~NISTIR 8272, Impact Analysis Tool for Interdependent Cyber Supply Chain Risks [NIST20d]~~ NIST SP 800-161 – Supply Chain Risk Management Practices [NIST15b] .
5/20/23	State Audit Working Group (SAWG)	2.0	14.3-C	The voting system's documentation must include the hardware and software information for all ~~the critical~~ components defined in the 14.3-B and at minimum list the following information for each component:	Even non-critical components can later be discovered to be non-trustworthy.	Accept	Accepted in principle. Needs to be reworded if the intent is to contain all components.	Partial Accept, See suggested edits.	For 14.3-C, Add related requirements 3.1.1-C and include in discussion using the list from 3.1.1-C to identify the Critical Components.
6/7/23	Free Speech for People	2.0	14.3-C	Recommended change: replace "critical" with "every component in the system." The Bill of Materials must not be limited to critical components as non-critical components may factor into malfunctions or contain security vulnerabilities that impact the entire system.		Accept	Accepted in principle. Needs to be reworded if the intent is to contain all components.	Partial Accept, See suggested edits.	For 14.3-C, Add related requirements 3.1.1-C and include in discussion using the list from 3.1.1-C to identify the Critical Components.
6/21/23	Smartmatic	2.0	15.1-D	the Table entry "Both normal and abnormal device shutdowns and restarts." should be modified to state "...where possible."	Not all abnormal shutdowns (device freezes) can be logged. The VSTL should check the code to ensure that the system is checking, upon start up, for evidence that the last shutdown was abnormal, then logging that indication once the logging facility is available in the start-up process.	Accept	This will need to be reworded, and possibly have a test assertion associated with it.	Reject	Consider including in a test assertion that it is logged in real-time or upon subsequent restart.
3/6/23	EAC	2.0	15.3-B - Updatable malware protection mechanisms	Review and look how this may apply to COTS packages, such as Operating Systems, that are no longer supported by their manufacturers.		Accept	Requires further investigation		
6/21/23	Smartmatic	2.0	Glossary	Please provide some detail to the definition of "voting device".	The current definition is circular and perhaps overlaps "vote capture device".	Noted	This should be looked at.		Voting Device could be replaced with "voting system" or "voting

Attachment 1 - 2023 Proposed VVSG Changes

Date	Organization	VVSG	Requirement	Proposed Changes / Additions *Note that red indicates an addition to an existing requirement, and strikethrough indicates removal from an existing requirement.*	Comment / Reasoning	EAC Initial Decision	EAC comment	NIST Initial Decision	NIST Comment
6/21/23	Smartmatic	2.0	General	New CDF standards are being published by NIST. Is there a policy around their inclusion in VVSG?	Recommend establishing an effectivity policy for new CDF's.	Accepted	Only CDFs in the VVSG are required. New CDF publications will need to be added to a future VVSG revision in order to be required.	Agree with EAC decision	
6/21/23	Voting Works	2.0	TA32B-1-1	This test assertion requires that "a cryptographic hash function MUST be used" to verify "that ONLY certified software is installed on the voting system." However, "a cryptographic hash function" is severely underspecified and could include known broken hash functions like MD5 that could produce a matching hash even if non-verified software was present. At the minimum, a standard like FIPS 180-4 should be required, but a better test would be something like dm-verity on Linux systems, which provides a Merkle tree attestation of the whole file system at once, robustly guaranteeing that the contents of the disk match only certified contents.		Requires further investigation.	Standard such as FIPS 180-4 may be a good idea. This may belong in a Test Assertion rather than VVSG 2.0	See suggested edits.	Consider updating the TA to require use of a NIST approved cryptographic hash function - FIPS 180, FIPS 202, or SP 800-185
6/21/23	Smartmatic	2.0	various, including "failure" (Glossary), and Test Assertion TA2.7-K 3	Where unit failure criteria is specified, especially the ubiquitous "Loss of data", this term is used multiple times in VVSG 2.0 but unlike previous VVSG versions, is less well defined. The VVSG 1.0/1.1 definition regarding votes/vote data confirmed to the voter would continue to be a useful definition for VVSG 2.0.	Recommend adding it to VVSG or to the Test Assertions. Similarly, "failure" and "human intervention" need to be considered in concert with "loss of data" and the definition of "failure" in the Glossary harmonized with related terms used in VVSG (and the Test Assertions". For example, if a unit undergoing ESD power cycles but reboots normally and without loss of data (allowed under current VVSG and associated Test Assertion), but needs a password to get to a polls open state (for ESD, ready to test), does that constitute "human intervention"?	Accepted / Noted	Failure should not need to be defined. Human Intervention may need to be defined.	Agree with EAC decision	Agree that previous glossary terms defined related to "failure" could be integrated into the VVSG 2.0 glossary for this case as appropriate.
8/2/22	Government Blockchain Association	2.0	N/A	New requirement needs to be added to accommodate remote digital ballot delivery, marking, and return. GBA-WG-20 Until the ballot is submitted, no marked ballot data is transmitted.		Reject	Out of scope. Remote Delivery, mark and return is outside of Voting Systems.	Agree with EAC decision	Out of scope
8/2/22	Government Blockchain Association	2.0	N/A	New requirement needs to be added to accommodate remote digital ballot delivery, marking, and return. GBA-WG-21 The correct ballot is delivered to (and only to) the eligible voter.		Reject	Out of scope. Remote Delivery, mark and return is outside of Voting Systems.	Agree with EAC decision	
8/2/22	Government Blockchain Association	2.0	N/A	New requirement needs to be added to accommodate remote digital ballot delivery, marking, and return. GBA-WG-22 The marked ballot is returned from only the voter who received the ballot.		Reject	Out of scope. Remote Delivery, mark and return is outside of Voting Systems.	Agree with EAC decision	Out of scope
8/2/22	Government Blockchain Association	2.0	N/A	New requirement needs to be added to accommodate remote digital ballot delivery, marking, and return. GBA-WG-23 The system will ensure that each and every marked ballot has been received and the act of receipt has been immutably recorded for tally & audit purposes.		Reject	Out of scope. Remote Delivery, mark and return is outside of Voting Systems.	Agree with EAC decision	
8/2/22	Government Blockchain Association	2.0	N/A	New requirement needs to be added to accommodate remote digital ballot delivery, marking, and return. GBA-WG-24 The voters' device must comply with the requirements of the Rules and Regulations of the Federal Communications Commission, Part 15, Class B [FCC19a]		Reject	Out of scope. Remote Delivery, mark and return is outside of Voting Systems.	Agree with EAC decision	Out of scope