Citizens' Oversight Projects (COPs)
771 Jamacha Rd #148
El Cajon, CA 92019
CitizensOversight.org
(619) 693-8960

support@citizensoversight.org

June 7, 2023

United States Election Assistance Commission
633 3rd Street NW, Suite 200
Washington, DC 20001

Attn: Testing & Certification
c/o: Paul Aumayr
phone (301) 960-1216
email: paumayr@eac.gov

REF: M1998

COPS Comments on VVSG 2.0

Dear Chair McCormick and Director Hovland:

We respectfully submit the comments below for the next iteration of the Voluntary Voting System Guidelines, referencing the VVSG 2.0 February 10, 2021 document.

Executive Director Raymond Lutz is an MSEE software engineer and the leader of our "AuditEngine" ballot image auditing platform. Through our ballot engine auditing work, we have gained substantial knowledge of the current voting machines and existing standards. Presently, we are collaborating with the IETF (Internet Engineering Task Force) SCITT (Supply Chain Integrity Transparency and Trust) working group which seeks to secure supply chain elements, including, primarily, the software supply chain. This work can also be applied to both election software and election data security. We are involved in this project to ensure the SCITT "Transparency Service" is suitable not only for election software, but also election data.

1. Introduction

In a nutshell, we are hoping to provide input which can be used to improve the specifics regarding election systems cybersecurity. Generally, the goal statements are present, such as the notion that all election data will be cryptographically signed. However, unless much more detail is provided, the signatures will be inconsistent and difficult to work with.

Importantly, it is essential to require that a third party check each signature to ensure that the software and data remain secure.

The move from paperless DRE (direct recording electronic) voting machines (that were the first response to the Help America Vote Act) to machines with a paper trail and better electronic records were an important step toward improving the security of our voting systems. Yet we need to take further steps, particularly with the realization that elections are a hostile environment, including malicious actors that, in theory, may even include the election officials.

Further transparency of the data and using traditional cryptographic mechanisms can move us to a much tighter and more auditable system, while acknowledging that moving away from touch-screen systems and to hand-marked paper ballots is essential. The voter can verify their votes, and auditors can verify that all options were fairly presented to the voter who uses hand-marked paper ballots.

The use of hand-marked paper ballots will, to some extent, quell the current call to move away from machines, while still allowing the necessary assistance of machines that are very good at counting and tracking yet recognizing humans are better at interpreting voter intent on a single ballot.

We don't support the notion that we should "ban all machines", but we must admit that there is some truth to the dismay that voters may feel when confronted with touch-screen machines that do not provide a ballot sheet with their votes to read.

The proposals below provide one way to improve voting systems, while we also acknowledge that these proposals are incomplete and will require further work to nail down all the details so they are fully interoperable. To achieve interoperability, we need consensus-based discussions on the details. Then, NIST can help codify the standards agreed upon.

This submission is based on this version of the VVSG 2.0 document:

https://www.eac.gov/sites/default/files/TestingCertification/Voluntary_Voting_System_Guidelines_Version_2_0.pdf

And this request for comments:

https://www.federalregister.gov/documents/2023/03/09/2023-04783/voluntary-voting-system-guidelines-request-for-comments

TABLE OF CONTENTS

A NOTE ON WRITING STYLE

Generally throughout this document, we will use "programmer" style (and straight, not curly) quotes, which always frame the terms and do not include punctuation. Numbers are always shown in numerical form and commas will always be included in conjunctive lists.

2. Improved Cybersecurity has been ordered

The President issued Executive Order (EO) 14028 on Improving the Nation's Cybersecurity on May 21, 2021[1]. We should notice this executive order was released after the current version of the VVSG was released, so this is a new and important influence on our work here.

This snippet from the order sums it up:

> The Federal Government must bring to bear the full scope of its authorities and resources to protect and secure its computer systems, whether they are cloud-based, on-premises, or hybrid. The scope of protection and security must include systems that process data (information technology (IT)) and those that run the vital machinery that ensures our safety (operational technology (OT)).
>
> It is the policy of my Administration that the prevention, detection, assessment, and remediation of cyber incidents is a top priority and essential to national and economic security.

The Department of Homeland Security Secretary Jeh, in a Jan 6, 2017 news release[2] said:

> I have determined that election infrastructure in this country should be designated as a subsector of the existing Government Facilities critical infrastructure sector. Given the vital role elections play in this country, it is clear that certain systems and assets of election infrastructure meet the definition of critical infrastructure, in fact and in law.
>
> ...
>
> [E]lection infrastructure becomes a priority within the National Infrastructure Protection Plan. It also enables this Department to prioritize our cybersecurity assistance to state and local election officials
>
> ...
>
> Now more than ever, it is important that we offer our assistance to state and local election officials in the cybersecurity of their systems. Election infrastructure is vital to our national interests, and cyber attacks on this country are becoming more sophisticated, and bad cyber actors – ranging from nation states, cyber criminals and hacktivists – are becoming more sophisticated and dangerous.

[1] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[2] https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical

The order specified that "critical software" was to be defined by NIST. They defined the term in the white paper "Definition of Critical Software Under Executive Order (EO) 14028"[3], briefly:

> **EO-critical software** is defined as any software that has, or has direct software dependencies upon, one or more components with at least one of these attributes:
>
> - is designed to run with elevated privilege or manage privileges;
> - has direct or privileged access to networking or computing resources;
> - is designed to control access to data or operational technology;
> - performs a function critical to trust; or,
> - operates outside of normal trust boundaries with privileged access.

The Whitehouse further released in March 2023 the National Cybersecurity Strategy[4] which states that:

> Cybersecurity is essential to the basic functioning of our economy, the operation of our critical infrastructure, the strength of our democracy and democratic institutions, the privacy of our data and communications, and our national defense.
>
> ...
>
> We must make fundamental changes to the underlying dynamics of the digital ecosystem, shifting the advantage to its defenders and perpetually frustrating the forces that would threaten it. Our goal is a defensible, resilient digital ecosystem where it is costlier to attack systems than defend them, where sensitive or private information is secure and protected, and where neither incidents nor errors cascade into catastrophic, systemic consequences.
>
> ...
> Defending the systems and assets that constitute our critical infrastructure is vital to our national security, public safety, and economic prosperity. The American people must have confidence in the availability and resilience of this infrastructure and the essential services it provides. We aim to operationalize an enduring and effective model of collaborative defense that equitably distributes risk and responsibility, and delivers a foundational level of security and resilience for our digital ecosystem.

3. The response to this order has been inadequate

The VVSG 2.0 must be updated to adequately address these concerns. Also, vendors should be encouraged to back-fit existing systems with improved cybersecurity, as most of it can be accomplished with software changes.

[3] https://www.nist.gov/system/files/documents/2021/10/13/EO%20Critical%20FINAL.pdf

[4] https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

Thus, these comments will provide a concrete direction that won't get bogged down with untested innovations that are required for end-to-end (E2E) verified systems. These suggestions can be easily integrated with voting systems that exist and traditional voting methods, and, most importantly, can be easily integrated with systems using hand-marked paper ballots.

4. Summary of our Points:

4.1 Improve Cybersecurity of Election Systems

We suggest a direction that leverages the existing and the respected FIPS 140-2. Since we are not claiming that this meets the "Properties of E2E Verified systems", particularly with respect to receipts, we still can make progress and comply with Executive Order 14028. The details, including the context and recommended changes to the VVSG of these comments can be found in both Appendix 1 and 4.

Our document "Improving Election Systems Cybersecurity" -- is included as an important part of our comment.

https://docs.google.com/document/d/1vZYATrxiA6vJ-2azdLG2jqOqXTDn7s68RotEFJeeByo/edit?usp=sharing

a. **Require a hardware implementation of a Trusted Platform Module which implements FIPS 140-2 (See Appendix 4)**

This requirement was watered down for vendors by allowing software implementations, and for E2E verification systems, no compliance at all. We disagree with this watering down and departure from the tried-and-true FIPS 140-2. A hardware implementation of a Trusted Platform Module can generate and protect private keys from everyone, including manufacturers and election officials, while other approaches are not as strong. Even if vendors are given a temporary pass, there should be a rating scale, and those machines that incorporate a hardware module should have a higher rating so local government agencies can differentiate on this basis. A hardware implementation should be preferred, and required in the future.

Therefore, this should NOT be watered down, and instead strengthened.

b. **Truly private keys that no one knows outside the device**

Such a hardware Trusted Platform Module must be able to internally generate random numbers based on a noise source with a minimum specified entropy and the ability to generate standard public and private key pairs, such that the private key is available to no one, and is infeasible to obtain even if the voting machine falls into the hands of fraudsters.

c. **Trusted Execution Environment (TEE)**

Ballot scanners, voter-facing equipment, and Election Management System (EMS) hardware should have a TEE (Trusted Execution Environment) which must run independently from the rest of the system, and provides FIPS 140-2 services and can check the integrity of the system outside the TEE. This is not mentioned in VVSG and it should be. Again, vendors that provide a TEE in their hardware should be differentiated from those that do not.

d. **Hardware Is Commonly Available at low cost.**
This hardware support for cryptographic security is now a commonly available aspect in many chip sets at low cost, and are even available in cloud-based systems using "Data Enclaves". Thus, to omit a hardware FIPS 140-2 implementation and to allow only software implementations can no longer be sustained given the Executive Order.

e. **Details of our Proposal "Improving Election System Cybersecurity"**
Initial details of our proposal are provided in the companion document "Improving Election System Cybersecurity", which is provided with a link in this comment. This document provides the outline of the methodology but, admittedly, is not in final form. We hope we can work with the EAC and NIST to complete and move this forward as a consensus-based standard.

This proposal is based on securing the very first unprocessed data artifact, the ballot image, using the internally generated private key of the scanner device and communicating with the host EMS using a communication standard that effectively implements a secure "sneakernet" called the "TransGapProtocol" TGP.

https://docs.google.com/document/d/1vZYATrxiA6vJ-2azdLG2jqOqXTDn7s68RotEFJeeByo/edit?usp=sharing -- "Improving Election Systems Cybersecurity". This document is an important part of our comment.

4.2 Define "Air Gapped" and work to adopt the TransGapProtocol TGP, for securing data for movement to, from, or among air gapped systems using removable media.

a. **Define "Air-Gapped" in the VVSG Glossary.**
Election systems are required to exist in an "air-gapped" configuration. Yet, despite the term being used many times in the body of the VVSG, the term is

not in the glossary. (See Appendix 2, below.)

b. **Adopt TransGapProtocol (or equivalent), for securing data for movement to, from, or among air gapped systems.**
Data must be moved between the EMS (election management system) and voting machines, which are also air-gapped, yet the exact protocol for communicating with those systems is left open. How does the EMS know the data is from the provisioned voting system and not from an imposter? How do we know that the data has not been changed in the device? Saying that the data is "encrypted" and "signed" is easy to add the text of the VVSG to "check the boxes" but it is not adequately defined.

The concept of the "TransGapProtocol" (TGP) is provided in our companion document "Improving Election System Cybersecurity", in the link provided above. The protocol, as described in the companion document, goes beyond ad-hoc methods normally known as "sneakernet".

TGP does still need development to adapt the concepts to the requirements of election systems, so this will take some effort to complete.

c. **Improve tracking and reporting of flash memory devices.**
We find that VVSG does not mention any requirements for tracking the flash devices to make sure they are all read by the EMS. We have found this to be lacking in the EMS software and a source of some errors when not all devices are read in. The TGP features cryptographically secure mechanisms to track and confirm that all devices have been accounted for. First, the secured list of all the public keys of all the scanner devices is published before the start of the election, and second, the results from all machines are published. This provides complete tracking of all devices.

d. **Use the "TransGapProtocol" for transferring data out of the system**
At the end of the election, the data must be transferred out of the air-gapped EMS system and provided to the public. TGP should be used for that as well, so it can be proven that the data came from the EMS and was unaltered.

e. **Post to a Transparency Service**
Once the data is produced by the voting system, it should be posted to an immutable transparency service which will provide for trusted time stamping for when the data was published, such that it cannot be altered later. This includes the incremental data releases of signed ballot image data, as recommended by our companion document "Election System Cybersecurity". The work being done by the IETF SCITT (supply chain integrity, transparency and trust) promises to be a good match for this application.

4.3 Improve minimal standards for Hand-Marked Paper Ballots

a. **Hand-Marked Paper Ballots must be the primary focus**
We now realize that hand-marked paper ballots are unsurpassed for voter verifiability (as the voter witnesses their own marking of the ballots with their hand) and auditability (as the set of options offered to the voter in their private voting session are documented on the sheet, unlike all forms of BMD touch-screen interface).

We offer the paper "Guidelines and Terminology on the Ease of Voter Verification"[5] to support our comment in this regard.

b. **Define "Hand-Marked Paper Ballot" in the glossary**
The glossary does not currently define "Hand Marked Paper Ballot" and instead defines "Manually-Marked Paper Ballot" which is not in popular use, and is not used elsewhere in the document, whereas "Hand-Marked Paper Ballot" is used multiple times, and is the normal nomenclature. See the corresponding Appendix for details.

c. **Define a standard format for a Hand-Marked Paper ballot, and develop criteria for how these are used.**
Despite widespread use in various vendor-specific formats, there is no standard definition for the layout and style encoding (style barcode) that is used for hand-marked paper ballots. It will help to have a standard format for interoperability, auditing, and voter education.

We therefore submit the companion document as a starting point for this discussion, "Hand-Marked Paper Ballot Standard"[6]. See the corresponding Appendix for details.

Please note that this standard does not restrict the formatting of the content of the ballot but only the frame and technical characteristics, including a barcode that expresses the district, data, style, precinct, and page with error detection, and the orientation of the sides of the ballot for best probability to avoid bleed-through hazards when targets are placed in the same location on each side.

[5] Guidelines and Terminology on the Ease of Voter Verification
https://docs.google.com/document/d/1Qz9Iin4AwzwNxVPHPoZZmV9W0EfQp5JcdSN6JqEAErM/edit?usp=

[6] Hand-Marked Paper Ballot Standard
https://docs.google.com/document/d/1H898yQcvzBAhZwqPtZpXSkFmxz3kkAkjBdKOYKcnnjg/edit?usp=sharing

4.4 Continue to refine the CVR standard to provide a more usable data format.

a. Another round of discussion on the "Common Data Format, Cast Vote Record" standard should occur.

b. Although we support the use of a common data format for the cast-vote record, we have found the currently approved format is difficult to use and is not thrifty in terms of size of the file(s) generated, their complexity, and ease of use.

c. We believe a flat data format, rather than the tree style format would be a better match, and XML should not be the primary data encoding method, as it is a very wasteful format and is now on the decline.

d. Section "**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.

e. The current CVR "CDF" as proposed by NIST (and most particularly implemented by Dominion) has the following weaknesses:

i. Results in a very large file or numerous file(s), commonly broken down by batch. In San Francisco, this results in over 13,000 individual JSON files.

ii. There is no master file to keep track of all the subsidiary files.

iii. A given record provides the ultimate resolution of the vote on each contest, but not the density of the original marks, particularly on options that were not resolved to votes. For example, if the record shows a vote for Candidate A but not Candidate B, the information about the marks for Candidate B are not included.

iv. If a contest is marked as overvoted, the information regarding which marks were voted is not available at all, including the mark densities of the options that were determined to be selected and resulted in the overvote.

v. If the ballot is adjudicated, there is no way that an individual contest can be marked "verified" if it is unchanged. If a contest is changed during the adjudication process, then obviously we know that the adjudicator checked that contest. But there is no way to tell if other contests that were unchanged were also adjudicated. Also, if the adjudication checked the ballot and confirmed one or more contests, there is no way to tell because no adjudication record will be created.

vi. Thus, we find that many election offices mark contests as "undervoted" when in fact they were overvoted, to allow them to keep track of whether all overvoted cases were reviewed and confirmed.

vii. The TransGapProtocol (TGP) or equivalent is not specified.

4.5 Sections on E2E Verifiable Voting should be moved to an appendix until such systems have been defined and approved.

No other *uncertified* voting system is included in the VVSG and there is no reason that E2E voting systems should be an exception. All sections about E2E should either be removed completely from the VVSG or moved to an Appendix. (Those working on the development of an E2E system have acknowledged it is far from ready for certification review – even after 10 years of work. Due to the innate challenges within the system and the non-transparent nature of the system, it likely will never be certified,)

The current VVSG 2.0 says

> "Due to the lack of E2E verifiable voting systems available within the current market, there are no verified E2E cryptographic protocols. A standard public process for approval of the E2E cryptographic protocols will need to be established outside of the VVSG. Once this process is established, the VVSG requirements can point to the approved/verified cryptographic protocols as acceptable for use within an E2E verifiable voting system.

The EAC has announced the "End To End (E2E) Protocol Evaluation Process" which is outlined on the webpage on the EAC.gov website: https://www.eac.gov/voting-equipment/end-end-e2e-protocol-evaluation-process

It is here that we learn of the "Properties of cryptographic end-to-end verifiable voting protocols" (but these are not listed in this manner in VVSG 2.0):

- **Cast as Intended:** Allow voters to confirm the voting system correctly interpreted their ballot selections while in the polling place via a receipt and provide evidence such that if there is an error or flaw in the interpretation of the voters' selections.

- **Recorded as Cast:** Allow voters to verify that their cast ballots were accurately recorded by the voting system and included in the public records of encoded ballots.

- **Tallied as Recorded:** Provide a publicly verifiable tabulation process from the public records of encoded ballots.

Although more than two years have elapsed, there still are no verified protocols and we had only one public meeting where some presentations were provided. At this public meeting, there were serious questions as to the viability of the initiative.

E2E cryptographic protocols have not been approved and the detailed public process for approving them has not been established. More importantly, the ideas for these systems are built on the notion that ballots and ballots selections will be completely encrypted, and thus then we must rely on other software to validate the votes. We believe these systems of this type are not possible within the constraints of the goal of "software independence", and further, that they will not be accepted by the public due to the calls to "ban all machines", for example.

In an email from CitizensOversight to the EAC, we asked Paul Aumayr at the EAC about this and he said (on June 6. 2023):

> The EAC, with NIST, are presently looking at conducting a research study with state and local election officials. This is to better understand what those election officials believe are desirable properties of technology and supporting processes, and to increase voter trust. After that, it would likely be necessary to investigate whether E2E systems offer the properties that address election officials' concerns. It is estimated that such a study would likely take about 18 months. It should also be noted that funding for such a study would need to be approved first.
>
> In answers to your other questions:
>
> - There has not been any further discussion by mailing list.
> - A working group has not been formed.
> - The criteria has not been further refined.
> - There have not been any submissions.

Meanwhile, we note that there are elements of election systems that *are already* deployed that *are not even addressed* in the VVSG, such as e-pollbooks, remote voting systems, and ballot printing on demand.

Thus, the entire section "9.1.6 – Cryptographic E2E verifiable", and other references should be at least moved to an appendix until these systems are actually shown to be viable.

Making this a central part of the VVSG makes it seem that these protocols are real, and that they will solve the cyber security issues in conventional voting systems. Unfortunately, we have reviewed these systems and find that in the most prominent proposals, they are a substantial departure from voting methods used today, are not easily scalable, have their own set of failure modes, and in our opinion, will not be acceptable to the public.

Clearly, a great deal of effort has gone into including provisions for E2E verifiable voting systems, and some of the implementation attempts have consumed many millions of dollars of development. At the same time, traditional cybersecurity mechanisms are only specified as a goal, such as "all data should be cryptographically signed", but without additional detail and standards for how the signatures are used. The lack of specific protocols makes this statement insufficient. Signatures that no one checks are worthless; each signature must be checkable and checked by a third party.

Therefore, we suggest that the VVSG attend to improving cybersecurity per the Executive Order mentioned, rather than continue to pursue the E2E systems that have not been demonstrated to be scalable and, most importantly, that they will be accepted by the public.

Moving "9.1.6 – Cryptographic E2E verifiable" to the appendix should also be paired with a review of the goals of such a system, with the intention that progress can be made perhaps without accomplishing all the goals as originally specified. For example, E2E verified voting systems have the underlying notion that a receipt can be given to the user. Perhaps this constraint can be loosened and no receipt is provided to the user but the data flow can be fully secured and reviewed. It is our evaluation that the current "properties" of such futuristic systems were guided by some existing ideas and cherished technical papers, such as homomorphic encryption, rather than a more general goal of improving the cryptographic security of voting systems.

See APPENDIX 1. Additional Comments On "E2E Verified Voting Systems" for detailed recommendations on the sections to move to an Appendix of the VVSG and some changes to make to those sections.

5. Conclusion

This completes our comments on VVSG 2.0. Included in our comment are the following companion documents:

1. **Improving Election Systems Cybersecurity** -- This proposal is based on securing the very first data artifact in a typical voting system, the ballot image: https://docs.google.com/document/d/1vZYATrxiA6vJ-2azdLG2jqOqXTDn7s68RotEFJeeByo/edit?usp=sharing

2. **Guidelines and Terminology on the Ease of Voter Verification** -- https://docs.google.com/document/d/1Qz9Iin4AwzwNxVPHPoZZmV9W0EfQp5JcdSN6JqEAErM/edit?usp=

3. **Hand-Marked Paper Ballot Standard** -- https://docs.google.com/document/d/1H898yQcvzBAhZwqPtZpXSkFmxz3kkAkjBdKOYKcnnjg/edit?usp=sharing

Respectfully submitted,

--Ray Lutz
Executive Director, Citizens Oversight
raylutz@citizensoversight.org

Endorsements:

Ray Lutz, Representing Citizens Oversight (COPS)

Ruth H. Strauss, MD

Darlene Little, Member of COPS, Scrutineers

Paul Burke, VoteWell.net

Garrett Lutz, San Diego

Madge Torres, Board Member

Lianda I. Ludwig, AUDIT USA, San Diego, CA

John Brakey, Arizona

APPENDIX 1. Additional Comments On "E2E Verifiable Voting"

In support of 1. "Sections on E2E Verifiable Voting should be moved to an appendix"

1. **E2E Verifiable voting" properties are inappropriate**
   "E2E Verifiable voting" properties for protocols are too restrictive, and do not allow for near-term improvements in the security of voting systems. These current requirements do not cover most issues that cause doubt in the results. Voters are not as concerned that their ballot selections have been correctly interpreted ("Cast as intended") and that their cast ballots has been correctly recorded ("Recorded as cast") but are more concerned that additional ballots have been added in (i.e. not "their" ballots) or that the machines may alter ballots that are not identified as "theirs". Furthermore, the requirement that voters can find and check their ballot stands in contrast with simultaneous requirements for voter privacy. Of course, we support the “tallied as recorded” attribute, and we wish this aspect was fleshed out a bit more, to address the various hazards (vulnerabilities for hacking or mistakes).

2. **Progress can be made without meeting the E2E Verifiable Voting goals**
   The Executive Order 14028 pushes for more security of critical infrastructure. Certainly, voting systems are critical infrastructure. We believe there is a lot of progress that can be made without meeting the first two E2E properties, and without changing the mode of voting or dramatically changing voting machines.

3. **The E2E Verifiable Voting properties are not general enough**
   These properties were established with specific systems in mind, such as homomorphic encryption, and other methodologies that encrypt the vote but allow for it to be tabulated. These systems are inherently difficult to scale, because they encode each vote (each target 0 or 1) separately and expand the number of bits that are to be processed from 1 to 4096 for each option, and makes it hard to track and test because everything is encrypted. Now we admit that there may be other methodologies, but jurisdictions around the country are very large, with many ballot styles and contests. Encrypting each vote will not actually improve the manageability of the data, it will lead to potentially losing track and allowing ballots to be easily added to the mix without anyone noticing.

   Encrypted data is hard to track. This is obvious. If you can easily read it and make sense of it, then you can constantly check it and make sure things are operating correctly. With encrypted data, design errors are easy to make.

   A related story is about two design teams that were working together to simulate incoming ballistic missiles that were predicted to come in over the north pole. When the two teams got together, they realized something was wrong with the data, but they did not know what. Once they created visualizations of their work, they finally could see the problem. One team used 0 degrees using navigational references, where 0 means north, 180 south, 90 east and 270 west, while the other group was using mathematical references, where 0 degrees is along the x-axis, and thus east. It took transparency and visibility to finally get to the bottom of this. Encryption of the data does not help us ensure that no avoidable mistakes are being made.

What happens if there is a problem with the E2E code? If the data is decrypted, then there is a very good chance that voter identities can be revealed, because they are carried with the ballot data in at least some of the systems outlined. But indeed since no systems have been actually submitted, we can only guess what they will ultimately do, but providing receipts and allowing the voters ballot to be looked up does provide a way for someone to derive the linkage[7].

4. **Systems that meet E2E Verifiable Voting properties will not improve voter confidence**
   We believe that even if E2E systems were produced that meet these goals, we do not believe they will improve voter confidence. This is because the systems we have seen so far are based on BMD (ballot marking device) technology, which does not actually provide the summary of the voter's selections on the ballot that was cast. Rather, the voter must trust that, in the final round, they were submitted as cast. Thereafter, the vote is encrypted, and no one can review whether the vote has been correctly recorded or tallied unless they have a high level degree in math and can conduct complete mathematical proofs to show that the vote of the ballots is consistent. This need for extensive software to track the vote in the system forces these systems to not be "software independent".

5. **Recent Failures would not be detected**
   The recent failures in Antrim County, MI in the 2020 General Election and the DeKalb County, GA May 24, 2022 primary election, where the slate of candidates was changed at the last minute (in DeKalb, one candidate dropped out late) or the contests on the ballot were corrected (as in Antrim County, MI), the interpretation of the vote on the ballot was different, and in the case of DeKalb, the hand-marked paper ballots were processed correctly, but the BMD ballots were not. In that case, voters were allowed to vote for the dropped candidate, and it appeared on the ballot, but it was later removed, but in the process, the other candidates were misinterpreted.

   In such a case, the mathematical proofs may be good all the way through, and yet it

[7] See section 2.4 of the Helios protocol, although no systems have been formally submitted for review, this system is similar to the "ElectionGuard" system being developed by Microsoft https://www.usenix.org/legacy/event/sec08/tech/full_papers/adida/adida.pdf

might be that no one would notice that the bits are for the wrong candidate. In other words, the homomorphic encryption used by at least one of the prominent E2E proposals makes catching this error even less likely. This sort of configuration error is easy to make and there is no encryption on earth that can tell what the proper list of candidates is. Fixing this issue has nothing to do with E2E systems, because encrypted errors are still errors.

In fact, it would be a serious step in the wrong direction if the systems that have been proposed currently ever get any traction, because we believe this type of error would be much more difficult to track down.

6. **BMD Type Interface is not Verifiable or fully auditable**

   The BMD touch-screen type interface is not verifiable. Certainly, the voter can read what is printed on the ballot summary card, but it is not possible to know what was provided to the voter in their private voting session. The best user interface for both the voter and for later auditing is the hand-marked paper ballot[8].

   There is a great deal of consternation today about "machines" involved in the election process. We believe that using hand-marked paper ballots will alleviate most of these concerns because voters interact with paper and pen and hand-countable paper ballots while still allowing machine processing. The E2E systems we have reviewed, and what is apparently contemplated by the "properties" of such systems, also have the same problems mentioned above in the BMD interface. The E2E systems do not provide for any verifiability of what the voter was presented nor do they use hand-marked paper ballots. A hand-marked paper ballot is the only type which demands that the voter simultaneously verify what they are voting on, and provide to auditors that all the options were shown to the voter.

7. **Transparency is Vitally Important**

   Instead of encrypting the vote and making it extremely difficult to track, we believe using hand-marked paper ballots and securing the ballot images, while anonymizing the ballots will accomplish the overall goals of E2E verifiable voting systems. This will not, unfortunately, comply with all the properties. We believe that maintaining transparency throughout the process is more important than obfuscating the vote through encryption.

These references in VVSG 2.0 are primarily targeting a E2E[9] voting scenario which utilizes direct voter entry using typically a touch-screen interface. Such voting systems cannot

[8] https://docs.google.com/document/d/1Qz9Iin4AwzwNxVPHPoZZmV9W0EfQp5JcdSN6JqEAErM/edit?usp=share_link -- Guidelines and Terminology on the Ease of Voter Verification

[9] https://en.wikipedia.org/wiki/End-to-end_auditable_voting_systems

verify that the voter was provided with all the contests and options in their private voting session, and therefore it is completely unverifiable. In contrast, hand-marked paper ballots provide full verifiability, because the voter actually makes the mark, watches it being made; the full slate of options are shown, and can be verified after the fact. All these factors are missing from touch-screen type voting systems.

Additionally, currently proposed (but not officially submitted) E2E voting schemes are typically based on tricky and somewhat questionable and hard to learn interactions with the voter during the private voting session. They then encrypt the voter's choices and compile the results using homomorphic encryption. Four officials are considered trusted to then decrypt the result[10]. It is beyond the scope of this paper to discuss the limitations of these proposals, but our review finds that they are difficult to scale and complicate the tracking of data through the system. To date, no E2E auditable or E2E voter verifiable systems have been submitted to the Election Assistance Commission for approval. 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.

THE FOLLOWING MENTIONS OF E2E VERIFIABLE VOTING SYSTEM SHOULD BE REMOVED FROM THE MAIN BODY OF THE VVSG AND MOVED TO 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. Comments for additions or strikeouts are highlighted. In some cases, if the reference to E2E is not the only reason for the provision, then it can be kept in the body of the VVSG and modified accordingly.

COMMENT: We will show our comments like this.

~~STRIKEOUT text~~ means this should be moved to an Appendix.

Italics indicates our additions.

6.2-A - Voter independence:

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.

Principle 9 -- Auditable:

[10] See https://vote.heliosvoting.org/ and https://www.electionguard.vote/ and review of the proposal: https://copswiki.org/w/bin/view/Common/M1991

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 - ~~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 their ballot selections. Voters will also be able to verify that their ballots are included in the tabulation results.~~

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.

9.1.1 – Software independence

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.~~

...

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.

9.1.2-A – Tamper-evident records

The voting system must produce tamper-evident records that enable detection of incorrect election outcomes, including:

1. capturing the contents of each vote at the time of each ballot's casting, and

2. recording detected errors in a tamper-evident manner.

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.

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.

Discussion

Voter-facing scanners and other vote-capture devices produce the paper records or other tamper evident electronic records. These records can be useful artifacts for post-election audits.

9.1.3-A – Records for voter verification

The voting system must provide individual voters the opportunity to verify that the voting system correctly interpreted their ballot selections.

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.

THE FOLLOWING ENTIRE SECTION SHOULD BE MOVED TO AN APPENDIX.

Our Comments are included as highlighted text.

9.1.6 – Cryptographic E2E verifiable

9.1.6-A– Verified cryptographic protocol

The E2E cryptographic protocol used by the cryptographic E2E verifiable voting system must be evaluated and approved through a public process established by the EAC.

Discussion

Due to the lack of E2E verifiable voting systems available within the current market, there are no verified E2E cryptographic protocols. A standard public process for approval of the E2E cryptographic protocols will need to be established outside of the VVSG. Once this process is established, the VVSG requirements can point to the approved/verified cryptographic protocols as acceptable for use within an E2E verifiable voting system.

9.1.6-B – Independent evaluation of E2E cryptographic protocol implementation

A cryptographic E2E verifiable voting system must undergo an independent evaluation to verify it correctly and securely implements an approved E2E cryptographic protocol.

Discussion

An independent evaluation can be performed by any entity outside of the voting system manufacturer. Example best practices include using guidance from the FIPS 140 series [NIST01, NIST19a], NIST SP 800-133 Revision 2, Recommendation for Cryptographic Key Generation [NIST20f], or NIST SP 800-175B, Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms [NIST20g]. The independent evaluation and cryptographic engineering best practices used can be documented and submitted.

Lessons learned from the analysis of the source code of the Swiss Post system shows the value in making this code available for public review. See "How not to prove your election outcome"

[Lewis19b], and "Ceci n'est pas une preuve" [Lewis19a].

9.1.6-C – Cryptographic ballot selection verification by voter

A cryptographic E2E verifiable voting system must:

1. be capable of providing evidence that an individual voter can use to confirm that the voting system correctly interpreted their ballot selections, while in the polling place; and

2. provide evidence such that if there is an error or flaw in the interpretation of the voters' selections, the evidence can be used for detection of the error or flaw.

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.

Discussion

This requirement addresses cast-as-intended verification, which is one of the principal components necessary to achieve end-to-end- verifiability [Benaloh14].

Interpretation is the process by which the voting system converts the voter’s contest option selections into the format used to store these selections. Therefore, this evidence must sufficiently prove the representation of the voter’s contest option selections in digital form matches the voter selections as provided to the system.

Giving voters the opportunity to verify the voting system stored their ballot choices correctly is a fundamental building block in an end-to-end verifiable voting system.

See “End-to-end verifiability” [Benaloh14] and “Usability is not Enough: Lessons Learned from

‘Human Factors in Security’ Research for Verifiability" [Kulyk18] for more information on the various implementations of this technique.

Related requirements: 6.2-A – Voter independence

7.3-G – Full ballot selections review

9.1.6-E – Ballot receipt

10.2.4-A – Voting information in receipts

9.1.6-D – Methods for cryptographic ballot selection verification

1. A cryptographic E2E verifiable voting system documentation must include: the method for the voter to use the evidence provided for ballot selection verification to verify the correct interpretation of their ballot; and

2. a list of known verification tools, their supplier, and how the verification tools are used.

Discussion

Voter intent verification often relies on external verification tools to assist voters in the verification step(s). These can be external verifiers, which is either a second device, a website of a trusted institution, or software running inside the polling location. The manufacturer must provide documentation explaining the verification options available to voters. If the jurisdiction is expected to provide the verification tool or service, this must also be documented.

Related requirements: 9.1.6-C – Cryptographic ballot selection verification by voter

9.1.6-E – Ballot receipt

A cryptographic E2E verifiable voting system must provide a voter with a receipt that allows them to verify that their ballot has been correctly recorded and tallied by the system. These receipts

1. must not display any ballot selections made by the voter;

2. must not enable the voter to prove their selections on the cast ballot to others;

3. must be represented in a publicly documented format;

4. may contain a unique identifier; and

5. are accessible, verifiable, and preserve voter-privacy.

Discussion

This evidence should fail to confirm a voter's ballot has been correctly recorded and tallied by the system if the ballot has been removed, tampered with, or its selections altered, added to, or removed.

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.

Related requirements:	6.1-A – Preserving privacy for voters
	6.2-A – Voter independence
	7.3-G – Full ballot selections review
	8.3-A – Usability tests with voters
	10.2.4-A – Voting information in receipts

9.1.6-F – Disputes involving ballot receipts

The cryptographic E2E verifiable voting system documentation must provide procedures for collecting, investigating, and adjudicating disputes from voters based on the contents of their ballot receipts.

Discussion

This documentation will include a process to address the scenario where a voter attempts to verify with their ballot receipt and believes there is a problem with their ballot receipt

Related requirements: 9.1.6-E – Ballot receipt

COMMENT: Ballot Receipts may result in significant misinformation campaigns that may be technically possible to clear up using mathematical proofs, but may never be feasible to convince the general public.

9.1.6-G – Evidence export

A cryptographic E2E verifiable voting system must:

1. be capable of exporting all evidence supporting ballot tabulation verification, and

2. provide the export in an open and consumable format.

Discussion

Most recorded-as-cast verification approaches require the public posting of the evidence at some point after all ballots have been aggregated and tallied. As required in the previous requirement, the evidence must not reveal how voters voted.

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.

9.1.6-H– Mandatory ballot availability

A cryptographic E2E verifiable voting system must be capable of exporting all encoded ballots for public posting.

Discussion

The public posting does not have to be provided by the voting system, but the voting system must provide the evidence such that it can be published, and the verification process made accessible to voters. The public posting of these exported encoded ballots is performed by election officials and is an essential part of the E2E verifiable process. It allows the public to verify the election results.

COMMENT: "encoded ballots" cannot provide any assurance to the general public because they are not human-readable.

9.1.6-I – Verification of encoded votes documentation

A cryptographic E2E verifiable voting system documentation must include:

1. the expected method by which voters will perform the ballot tabulation verification, and

2. how this method provides voters with the opportunity to verify that their ballots are included within the tabulation results.

Discussion

For example, a common method is to publish the evidence to a public bulletin board. The manufacturer should document this method or its alternative. The bulletin board, itself, might not be included in the scope of the voting system but the voting system must provide an export of the evidence to be published on the bulletin board.

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.

9.1.6-J – Verifier reference implementation

A cryptographic E2E verifiable voting system documentation must include:

1. a free publicly available reference implementation of a tool which can be used:

a. to verify evidence provided to a voter to prove that their ballot choices were correctly interpreted, and

b. to verify the evidence reported for voters to perform ballot tabulation verification;

2. the build instructions for the reference implementation, along with the tool.

Discussion

For the system to support the cast-as-intended property of end-to-end verifiable systems there must be at least one tool available to voters to verify that their ballot selections have been correctly interpreted. Additionally, for a cryptographic E2E system to be software independent, the voters need to have choices about what software to use and trust when performing verification. By providing an open source reference implementation may facilitate development of third-party verification tools.

COMMENT: The human eye is the most acceptable "tool" to voters.

Related requirements:	9.1.6-C – Cryptographic ballot selection verification by voter

9.1.6-K – Privacy preserving, universally verifiable ballot tabulation

A cryptographic E2E verifiable voting system tabulation process must preserve the privacy of every voter and provide a method for public verification.

Discussion

To be publicly verifiable, the approach provides a means for any auditor or observer to verify the correct decryption and tabulation of the votes (not necessarily in that order) using cryptographic proofs that are generated by the process.

Related requirements:	6.1-A – Preserving privacy for voters

END OF ENTIRELY MOVED SECTION
The remaining provisions are altered by removing E2E from their descriptions.

NOTE: ~~Strikethrough text~~ means these should be deleted from the main body of the VVSG and optionally move to an appendix.

Principle 10

Ballot Secrecy

The voting system protects the secrecy of voters' ballot selections.

~~10.2.1-B – Indirect voter associations~~

~~Indirect voter associations must only be used to associate a voter with their encrypted ballot selections.~~

~~Discussion~~

~~Certain channels of voting require indirect associations so that ineligible ballots can be removed before the ballot is read and counted. Some reasons include signature mismatch or death of a voter. The most common example of indirect association would be a randomly generated number. Best practice would ensure that indirect voter associations are only available to authorized election personnel.~~

~~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.~~

~~10.2.1-C – 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.~~

~~Discussion~~

~~Certain channels of voting require indirect associations so that ballots can be removed before casting for a variety of reasons including signature mismatch or death of a voter. These types of ballots are often considered provisional or recallable ballots.~~

~~Applies to: Cryptographic E2E verifiable voting system~~

COMMENT: The following should be instead treated as "provisional ballots" and they should be kept in a privacy envelope until they are cast, and then merged with other non provisional ballots.

~~**10.2.1-D – Isolated storage location**~~

~~Ballots that are not cast and contain an indirect association must be separated from cast ballots.~~

~~**Discussion**~~

~~Ballots that contain an indirect association are not considered cast. Cast ballots and ballots having their eligibility considered need to be kept separate from each other. Although not the only way of meeting this requirement, one example would be storing cast ballots in a different directory from ballots not yet cast.~~

~~Applies to: Cryptographic E2E verifiable voting architectures~~

COMMENT: Again this is regarding provisional ballots and may not need to be separately treated here.

~~**10.2.1-E – Removal of indirect voter associations**~~

~~The voting system must be capable of removing the indirect voter association between a ballot and a voter once that voter is determined to be eligible.~~

~~**Discussion**~~

~~Provisional or recallable ballots may require indirect associations so that ballots can be removed before casting. After a voter's eligibility is determined the indirect voter association can be removed and the ballot can be added to the collection of cast ballots.~~

~~In the case of electronic E2E systems, whatever data record provides this association must be removed from the system. Ballots with indirect associations are not considered cast until the association is removed. Best practice would ensure that indirect voter associations are only available to authorized election personnel.~~

~~Applies to: Cryptographic E2E verifiable voting architectures~~

~~**10.2.1-F – Confidentiality for ballots with indirect voter associations**~~

~~The voting system must only be capable of decrypting a ballot after any indirect voter association to it has been removed.~~

~~Discussion~~

~~Encryption of the ballot preserves the confidentiality of the voter's ballot selections while the ballot is tied to an indirect association to the voter. The indirect voter association is not encrypted with the ballot.~~

~~The voting system must not be capable of decrypting a ballot that still has an indirect association to a voter. A possible approach to implement this is by requiring that a decryption key (or set of keys) be entered to decrypt ballots but disallowing input until after all indirect associations have been removed. If the key is present on the system at the same time as indirect associations, it may be possible for malicious software to decrypt ballots and associate selections with voters.~~

~~Applies to: Cryptographic E2E verifiable voting architectures~~

~~10.2.2 – Identification in vote records~~

~~10.2.2-A – Identifiers used for audits~~

~~Identifiers used for tying a cast vote record (CVR) and ballot images to physical paper ballots must be distinct from identifiers used for indirect associations.~~

~~Discussion~~

~~For the purpose of these requirements, associations between physical ballots and CVRs are not considered direct or indirect identifiers.~~

~~Related requirements: 9.1.5-F – Unique identifier~~

10.2.2-E – Randomly generated identifiers

Randomly generated identifiers used for audits must use random bit generators specified in the latest revision of NIST SP 800-90 series on random bit generators.

Discussion

This requirement is important to ensure the use of a cryptographically secure pseudo-random number generator (CSPRNG) and also to ensure any random numbers, such as unique identifiers on a ballot, cannot be used to recreate the order in which a ballot was cast.

Recreating the order of cast ballots can cause ballot secrecy issues if a voter's ballot can be identified. To ensure voting system vendors are following the random number generation recommendations in the 800-90 series, they will need to submit to the Cryptographic Module Validation Program (CMVP) and the Cryptographic Algorithm Validation Program (CAVP) for conformance testing.

For additional information, see NIST SP 800-90A Rev 1, Recommendation for Random Number Generation Using Deterministic Random Bit Generators [NIST15a] and NIST SP 800-90B, Recommendation for the Entropy Sources Used for Random Bit Generation [NIST18a].

Related requirements:	9.4-B – Random numbers supporting audit processes
	10.2.2-D – Aggregating and ordering

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.

~~10.2.4 – Voter information in other devices and artifacts~~

~~10.2.4-A – Voting information in receipts~~

~~Receipts produced by cryptographic E2E verifiable voting systems must not contain voter information.~~

~~Discussion~~

~~The voting system must not issue a receipt to the voter that would provide proof to another of how the voter voted.~~

~~13.3 - All cryptographic algorithms are public, well-vetted, and standardized.~~

13.3-A – Cryptographic module validation

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 FIPS 140[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.

~~13.3-B – E2E cryptographic voting protocols~~

~~Cryptographic functions specific to E2E cryptographic voting protocols must adhere to requirements set by the EAC and are omitted from FIPS 140-2 validation.~~

~~Discussion~~

~~The cryptographic E2E verifiable voting protocol used by the voting system is subject to the evaluation in requirement 9.1.6-B – Verified Cryptographic Protocol. Common place cryptographic operations used within E2E systems, such as encryption, decryption, and hashing, are subject to the FIPS 140 [NIST01, NIST19a] validation requirement.~~

~~\~~

~~Applies to: Cryptographic E2E verifiable voting systems~~

~~Related requirements: 9.1.6-A – Verified cryptographic protocol~~

13.3-C – Cryptographic strength

Devices using cryptography must employ NIST approved algorithms with a security strength of at least 112-bits.

> 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.

Discussion

At the time of this writing, NIST specifies the security strength of algorithms in SP 800- 57, Part 1 [NIST20a]. This NIST recommendation will be revised or updated as new algorithms are added, and if cryptographic analysis indicates that some algorithms are weaker than presently believed. The security strengths of SP 800-57 are based on estimates of the amount of computation required to successfully attack the particular algorithm. The specified strength should be sufficient for several decades.

This requirement is not intended to forbid all incidental use of non-approved algorithms by OS software or standardized network security protocols.

13.3-D – MAC cryptographic strength

The key used with Message Authentication Codes must also have a security strength of at least 112 bits and use a 96-bit tag length.

Discussion

Message authentication codes of 96-bits are conventional in standardized secure communications protocols, and acceptable to protect voting records and systems.

> 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.

13.3-E – Cryptographic key management documentation

The voting system documentation must describe how key management is to be performed.

Discussion

This document provides procedural steps that can be taken to ease the burden of key management and safely perform these operations.

COMMENT: The VVSG should define this in a standard way rather than allowing each voting system to do it differently.

13.4 - The voting system protects the integrity, authenticity, and confidentiality of sensitive data transmitted over all networks.

13.4-A – Confidentiality and integrity protection of transmitted data

COMMENT: The VVSG should define Air-Gapped and mention here as the preferred method.

The voting system must:

1. mutually authenticate all network connections;
2. cryptographically protect the confidentiality of all data sent over a network; and
3. cryptographically protect the integrity of all election data sent over the network.

Discussion

Mutual authentication provides assurance that each electronic device is legitimate. Mutual authentication can be performed using various protocols, such as IPsec and SSL/TLS. Only wired local area network (LAN) communication, such as ethernet, is possible for VVSG 2.0 voting systems. This requirement includes network appliances such as switches, firewalls, and routers within its scope.

This does not prevent the use of "double encrypted" connections employing cryptography at multiple layers of the network stack. Data, such as ballot images, must be encrypted before transmission.

Integrity protection ensures that any inadvertent or intentional alterations to data are detected by the recipient. Integrity protection for data in transit can be provided through the use of various protocols, such as IPsec VPNs and SSL/TLS. For more information about TLS implementations, see NIST SP 800-52 rev. 2, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations [NIST19b]

FROM THE GLOSSARY:

This can be moved to the Appendix, or left in the Glossary.

cryptographic end-to-end(E2E) verifiable voting systems

A voting system that uses cryptographic techniques to store an encrypted copy of the voter's ballot selections while maintaining ballot secrecy and allows election outcomes to be independently and universally verified by members of the public. These voting systems provide voters with a special receipt of their cast ballot—one that allows them to verify their vote was included in the outcome but does not reveal to anyone how they voted.

Synonyms: Receipt-based system

COMMENT: The term "Receipt-based system" is never used in the document. This entire definition can be moved to the Appendix until such systems are actually approved.

APPENDIX 2. Additional Comments On "Air-Gapped"

"AIR-GAPPED" is used but is not defined in the glossary. It should be a primary mechanism for security.

From Page 5:
To limit the attack surface on voting systems, the Guidelines require that any election system, such as an e-pollbook or election reporting system, be air-gapped from the voting system.

COMMENT: It is the Voting System that must be air-gapped. Other systems must have additional protections from internet abuse.

COMMENT: 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!

15.4-B – Secure network configuration documentation

The voting system documentation must list security configurations and be accompanied by network security best practices.

Discussion

This documentation may include how external network services are not included as part of the voting system and are handled through a separate air-gapped process. For example, a sneaker-net process may be used to manually transfer election results to another system that uses public telecommunications to transmit the unofficial election results to a central count center.

A variety of documentation providing secure configurations for network devices is publicly available from the US government.

If outside manufacturers provide guidance and best practices, these need to be documented and used to the extent practical.

This documentation may also include the use of firewalls and intrusion detection systems (IDS).

Firewalls and IDSs are typically used to control and monitor the boundary between a private network and the internet. Although the current requirements do not allow for internet connectivity, firewalls and IDSs may also be used for internal boundaries and monitoring inside a private network. Guidance for Intrusion Detection and prevention systems can be found in NIST SP 800-94: Guide to Intrusion Detection and Prevention Systems [NIST07].

Related requirements: 14.2-F – Secure configuration and hardening documentation

14.2-F – Secure configuration and hardening documentation

The voting system must follow a secure configuration guide for all underlying operating systems and other voting system components, with any deviations from the secure configuration guidance documented and justified.

Discussion

Properly configuring an operating system is a difficult and complex task, with small settings potentially causing a large impact. Industry, NIST, and various agencies within the DoD offer guidance for specific operating systems, as do OS and component manufacturers. Some examples include Security Technical Implementation Guides (STIGs) [DISA20] and the Center for Internet Security (CIS) benchmarks.

Documenting deviations ensures that important settings are not overlooked and decisions to deviate are properly considered.

Related requirements: 15.4-B – Secure network configuration documentation

COMMENT: The above section should mention air-gapped as a mechanism to achieve security.

APPENDIX 3. Additional Comments On "Hand-Marked Paper Ballot"

MISSING DEFINITION: hand-marked paper ballot

mentioned twice in the scope:

If a majority of voters utilize hand-marked paper ballots, a sufficient number of accessible voting stations (including alternative language ballot features) must be available in each polling place to ensure their consistent availability in case of malfunctions. A sufficient number of machine-marked ballots must also be produced by those voting stations to ensure non-discrimination and ballot secrecy, particularly when the ballots produced by the accessible voting system differ in size, shape, and/or content from the hand-marked ballots and are thus readily identifiable. Procedures and training for poll workers on the operation of the accessible voting stations are also necessary to support this usage.

7.2-J – Paper ballot target areas

On a paper ballot that a voter marks by hand, the area of the target used to mark a voting selection must be at least 3 mm (0.12 inches) across in any direction.

Discussion

This requirement applies to marking ovals, circles, squares, or other optical scan ballot designs.

Although the marking target for hand-marked paper ballots needs to be large enough to see, a target that is too large can also make it hard to fill in the area completely.

In Glossary:

batch-fed scanner

An electronic voting device that typically:

• accepts stacks of hand-marked or BMD-produced paper ballots and automatically

processes them until the stack is empty;

• is usually used at an election jurisdiction's central location;

• is mostly commonly used to process absentee ballots;

• usually has input and output hoppers for ballots;

Such a scanner may also optionally include the following functions:

• scans a ballot and rejects it if either unreadable or un-processable;

- detects, interprets, and validates contest selections;
- detects and sorts (either digitally or physically) ballots that are unreadable or unprocessable, or that contain undeterminable selections, marking exceptions, or writeins; and
- tabulates and reports contest results as required.

~~This unit was previously referred to as central count optical scanner or CCOS.~~

Synonyms: CCOS, central tabulator, central-count optical scanner, high-speed optical scanner

manually-marked paper ballot

Paper ballot marked by a voter using a writing utensil.

Synonyms: MMPB

COMMENT: Change this to use "hand-marked paper ballot, HMBP" as the primary definition and probably not use manually marked at all, as it is not used.

paper ballot

A piece of paper, or multiple sheets of paper, on which all **contest options** of a given **ballot style** are printed.

Synonym: Hand-Marked Paper Ballot

COMMENT: Please note that this definition does not allow ballot summary sheets, which do not provide all contest options of a given ballots style, but only provide the selected options.

We suggest that the definition allow for machine-marked paper ballots when they have the same format as the hand-marked equivalent.

post-election tabulation audit

A post-election audit that involves hand-counting a sample of (or all) votes on paper records, then comparing those counts to the corresponding vote totals originally reported:

- as a check on the accuracy of election results, and
- to detect discrepancies using accurate hand counts of the paper records as the benchmark.

ADD:
Post-election audits may also include machine-assisted audits, such as by independently rescanning paper records or utilizing secured ballot images and processing these with

independent software and then comparing with the official results, either as aggregated totals or ballot-by-ballot by using the Cast Vote Records (CVRs).

COMMENT: If all votes are included in the hand-count, this is still an audit. An audit may also include reviewing ballot images, particularly if they are secured using the cryptographic security mechanisms proposed.

APPENDIX 4. Additional Comments on FIPS-140-2

FIPS 140-2 and Platform Security Module mentions (other than in E2E section):

Principle 13 - Data Protection

~~• Clarifies that there are no hardware security requirements (for example, TPM (trusted platform module))~~

• Requires Federal Information Processing Standard (FIPS) 140-2 [NIST01] validated cryptographic modules (except for end-to-end cryptographic functions)

• Requires cryptographic protection of various election artifacts

• Requires digitally signed cast vote records and ballot images

• Ensures transmitted data is encrypted with end-to-end authentication

COMMENT: Making hardware security modules optional goes against improving cryptographic security and should be reversed per EO-14028. Please see our detailed description of Improving Election Cryptographic Security in the companion paper.

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.

13.2-A – Signing stored election records

Cast vote records and ballot images must be digitally signed when stored and before being transmitted.

Discussion

Digital signatures address the threat that the records might be tampered with when stored or transmitted. Cryptographic hashes do not sufficiently mitigate this threat, as election records could be altered and then re-hashed. Digital signatures also allow verification of the source of any created or modified records. Additional information can be found in FIPS 186-4 Digital Signature Standard [NIST13c].

COMMENT:
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.