Government Blockchain Association

Voting Working Group

Voluntary Voting System Guidelines (VVSG) 2.x

Supplement for Remote Accessible Ballot Delivery Marking & Return (RABDMR)

Date: August 2, 2022
Version: 1.0

Document Authors

Special thanks are extended to the individuals below for their content, review and valuable contributions to this document.

DeVote

- Eugene Morozov

Follow My Vote

- Adam Ernest

Government Blockchain Association

- Gerard Dache
- Susan Eustis
- Mark Waser
- Meiyappan Masilamani

L4S Corporation

- Paul Dowding

Prometheus Computing

- Frederick de Vaulx

The Global Strategy

- Tatiana Revoredo

Voatz

- Linda Hutchinson
- Philip Andreae
- Eric Landquist

Utah County

- Amelia Gardner
- Rozan Mitchell

Table of Contents

1 Introduction 1

1.1 Background 1
1.1.1 History 1
1.1.2 Challenge 1
1.1.3 Response 2
1.1.4 Audience 2

1.2 Decentralized Immutable Ledgers 2

1.3 Voluntary Voting System Guidelines (VVSG) 2.x Supplement 2
1.3.1 Purpose 2
1.3.2 Scope 2

2 Remote Voting Methods 3

2.1 Official mailed paper ballot & envelope 3

2.2 Voter-printed ballot & envelope 3

2.3 Fax ballot return 3

2.4 Email ballot return 4

2.5 File upload ballot return 4

2.6 Browser-Based digitally protected ballot return 4

2.7 App based digitally protected ballot return recorded on an immutable ledger 5

3 Voluntary Voting System Guidelines Principles 5

3.1 High Quality-Design 6

3.2 High Quality Implementation 6

3.3 Transparent 7

3.4 Interoperable 7

3.5 Equivalent and Consistent Voter Access 8

3.6 Voter Privacy 8

3.7 Marked, Verified, and Cast as Intended 8

3.8 Robust, Safe, Usable, and Accessible 9

3.9 Auditable 10

3.10 Ballot Secrecy 10

3.11 Access Control 10

3.12 Physical Security 11

3.13 Data Protection 12
3.14 System Integrity 13
3.15 Detection and Monitoring 13
3.16 Communications 13
4 Conclusions & Recommendations 14
4.1 Conclusion 14
4.2 Recommendations 14
End Notes 15

1 Introduction

The world is going digital and along with it, the way people are casting their votes. More and more, jurisdictions are allowing for remote electronic voting. However, two forces are on a collision course with each other. They are:

- Citizens increasingly distrust election officials, processes, equipment, and results
- Increased demand for remote voting due to:
  - public health concerns
  - higher mobility of voters (overseas military, remote employment, and international travel) and
  - an aging population with reduced access to in-person polls.

This causes voters to be skeptical of remote election methods including mail, email, fax, ballot uploads, and app-based voting methods. It is vitally important for the sustainment of democracy that we restore confidence in our elections, including our remote ballot delivery, marking, and return methods.

1.1 Background

1.1.1 History

Ever since the Civil War military personnel have been afforded the right to vote by mail. By the late 1880s states has extended the right to vote by mail under certain conditions. And, in 2000 Oregon became the first state to vote entirely by mail.

The 2020 election occurred during a pandemic when many states reconsidered their rules around remote voting. Today 75% of the US population can vote remotely by mail.[i]

As early as 1990 soldiers deployed during Operation Desert Storm were able to vote via phone/fax machines and during the 2006 election Connecticut, Maine, New Hampshire, Oklahoma, Oregon, and Vermont used vote by phone systems.[ii].

In 2018 Sierra Leone ran the first election using a remote technology that combined remote networking technology with advanced cryptographic security. They used blockchain technology to cryptographically record the votes to prevent tampering with or altering the election information. Since then, this technology has been used all around the world for local, state, and national elections.

Technology was being used to securely record those elections and could be protected from tampering with the votes of overseas personnel or those with disabilities.

1.1.2 Challenge

While some people challenge the security of digital ballot delivery, marking, and return, others dispute the integrity of mail in voting and other forms of remote ballot delivery, marking, and return. The United States Election Advisory Commission (EAC) has been vital in setting standards to allow election systems to be certified and enhancing the confidence in government election systems. The EAC has published the Voluntary Voting System Guidelines (VVSG). The VVSG describes the requirements that must be satisfied for a testing facility to certify and election

system. Unfortunately, the VVSG does not currently contain the appropriate requirements to certify a digital ballot delivery, marking, and return solution or system.

1.1.3 Response

This document was created by Government Blockchain Association (GBA) members who are election and technology experts. It is intended to make recommendations related to remote digital ballot delivery, marking, and return.

1.1.4 Audience

This report is written and being submitted to the U.S. Election Assistance Commission for consideration

1.2 Decentralized Immutable Ledgers

In the early 1980s researchers started exploring technology to verify the integrity of digital records. In 1982 David Chaum published a paper describing a system for establishing, maintaining and trusting computer systems by mutually suspicious groups. In the early 1990s Stuart Haber and W. Scott Stornetta implemented an immutable ledger using a chain of blocks that were connected by cryptographic links. And, later in 2008 the bitcoin whitepaper popularized the technology known as blockchain. Many advancements have been made since then. But one thing that has remained constant is that Decentralized Immutable Technology [1] creates new opportunities to ensure the integrity of election records. These technologies have been proven by the global adoption of cryptocurrencies. Today the ledgers that contain cryptocurrency records are used by untrusted parties to validate the ownership and status of billions of dollars of digital assets. This technology can now be used to validate the integrity of election records.

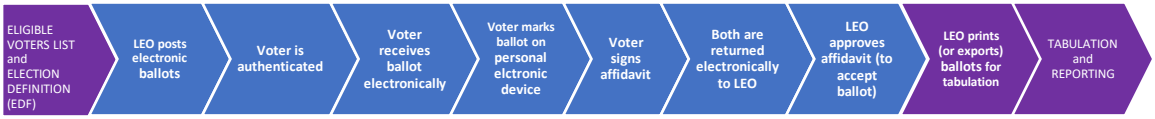
1.3 Voluntary Voting System Guidelines (VVSG) 2.x Supplement

1.3.1 Purpose

The purpose of this document to recommend changes to the VVSG to support remote electronic ballot delivery, marking, return, and storage.

1.3.2 Scope

The diagram below depicts the generic workflow for remote electronic voting, shown in blue.



Both in-person and remote voting require the list of eligible voters and election definition file of precinct and contest information to begin. Once marked ballots are returned, the local election official (LEO) assembles the ballots for tabulation and reporting. Acceptance and preparation of ballots for tabulation will vary slightly based on the seven remote voting methods presented.

[1] The term “Decentralized” is used intentionally as compared with “Distributed”.

2 Remote Voting Methods

All US jurisdictions offer some form of remote ballot return. Traditionally, this is an official mailed paper ballot. In addition, many states currently permit some form of electronic ballot return. The following seven methods are summarized below.

- Official mailed paper ballot & envelope
- Voter-printed ballot & envelope
- Simple fax ballot return
- Simple email ballot return
- Simple file upload ballot return
- Browser based, digitally protected ballot return
- App based, digitally protected and ledgered ballot return

2.1 Official mailed paper ballot & envelope

This method covers vote by mail of paper ballots to qualified voters. With this method, a voter will typically request an official paper ballot from their Local Election Official (LEO).

Voters then mark their choices on the official paper ballot and signs the affidavit. Voters return the marked ballot either by postal mail or authorized drop box. The LEO will review and approve the marked ballot and/or affidavit. Once approved, the marked ballot is ready for optical scanning and tabulation.

2.2 Voter-printed ballot & envelope

In this method, voters will print their own ballots before marking them for official delivery and tabulation. A voter will request a ballot to be electronically delivered to them. The LEO will authenticate the request by the voter based on local requirements and then electronically delivery the ballot to the voter.

The voter will mark the ballot electronically or by hand. Typically, the voters sign an affidavit and insert it along with their ballot in their own envelope.

Voters return the marked ballot either by postal mail or authorized drop box. The LEO will review and approve the marked ballot and/or affidavit. Once approved, the marked ballot is ready for optical scanning and tabulation.

2.3 Fax ballot return

There are some cases where registered voters can fax their marked ballot to the LEO. Typically, the voter will request access for digital return of hand marked or electronic ballot.

The LEO will conduct a voter verification and authentication based on identity management requirements. Prior to fax return, the voter either:

a. receives and marks ballot electronically then prints the ballot, affidavit (as needed) and envelope,
b. receives and prints the ballot electronically, marks it, signs affidavit.

The voter faxes (physical or eFax) to the jurisdiction's LEO with confirmation of delivery.
The LEO approves affidavit and separates it from the ballot. The LEO prints ballot and remakes ballot by hand to enable optical scanning for tabulation.

2.4 Email ballot return

There are more jurisdictions that allow voters to cast their ballots through email. As with other methods, the voter will request access for digital return of hand marked or electronic ballot. As in many jurisdictions, there is voter verification and authentication based on LEO's requirements.
The voter receives the ballot electronically through email.

The voter receives and marks ballot electronically and prints ballot, affidavit, and envelope; or in some cases the voter prints ballot, affidavit, envelope and marks by hand. Voter prints, signs and scans affidavit on their personal computers.
Unlike physical delivery, the voter attaches documents and returns via their personal email account.

Depending upon their jurisdictions, voters may obtain confirmation of receipt and/or review status. The LEO approves affidavit and separates from ballot. At this stage, the LEO prints ballot and remakes ballot by hand for optical scanning for tabulation.

2.5 File upload ballot return

As an alternative to emailing their ballots, voters can sometimes upload them to an authorized web portal site managed by a LEO. The process is somewhat similar to voting by email.

The voter requests access for digital return of hand marked or electronic ballot
Voter verifies identity and receives ballot electronically. Voter marks the ballot electronically and saves it to the computer (or prints and marks by hand.)
Voters will print, sign, and then scan the affidavit to their computers. Once the scanning is completed, then the voter authenticates (logs in to an authorized election website) based on LEO's requirements. Once logged in, the voter uploads documents to the web portal.
Voters may obtain confirmation of receipt and/or review status.

The LEO approves affidavit and separates uploaded to their web site. In many cases, the LEO prints ballot and remakes ballot by hand for optical scanning. As with other voting methodologies, the ballot is then ready for scanning & tabulation.

2.6 Browser-Based digitally protected ballot return

Some jurisdictions allow voters to cast their ballot using their web browser. This particular type of voting overlaps with email/ballot upload voting methods.

The Voter requests electronic ballot from their LEO. After proper authorization, the LEO sends an invitation to vote. A voter verifies identity based on LEO's requirements which allows them to receive and electronically marks the ballot.
The voter will in many cases electronically sign an affidavit. This step is based on jurisdiction requirements. This method of return permits supplemental or alternative advanced authentication techniques.

The ballot and affidavit are cryptographically protected and transmitted via electronic networks to the LEO's jurisdictional office. After a successful transmission, the voter receives a confirmation of receipt of submission. The LEO approves affidavit which enables viewing of ballot. The next step is for the jurisdiction to remake ballot for optical scanning. The ballots are then ready for optical scanning & tabulation.

2.7 App based digitally protected ballot return recorded on an immutable ledger

In recent years, more jurisdictions are enabling voters to participate in elections using their mobile device through a secure app. The number of vendors offering apps to deploy mobile-based voting is continuing to grow. This method of voting overlaps with email and browser-based voting but with some distinct differences.

Through their mobile device, the voter requests electronic ballot from their LEO. In turn, LEO sends an electronic ballot invitation to their registered/authorized voters.

The voter verifies their identity based on LEO's requirements programmed in the mobile app. The Voter receives and electronically marks the ballot in the app and then authenticates by electronically signing an affidavit. This step is based on jurisdiction requirements. This method of return permits supplemental or alternative advanced authentication techniques.

In this method of voting remotely through an app, the cryptographically protected ballot & affidavit are transmitted to and recorded on the jurisdiction's secure digital ledger.
The voter receives a confirmation of receipt of submission (voter may receive enhanced encrypted ballot confirmation.). The mobile app interfaces with the LEO's system of record to ensure that votes cast over a mobile app are tabulated and counted accurately.

3 Voluntary Voting System Guidelines Principles

The Voluntary Voting System Guidelines is a part of the national level voting system standards and published by the Election Assistance Commission. Adherence to these Guidelines is governed by state and territory-specific laws and procedures. The VVSG is used to support or facilitate the certification of election equipment.

The VVSG is organized around the following key quality attributes described in the sub paragraphs below that include our recommendations for changing the standards to enable remote election:

- Electronic ballot delivery
- Electronic ballot marking

- Electronic ballot return
- Electronic ballot storage

In their current form, these standards do not allow for the certification of remote electronic voting. Consequently, changes to the VVSG are needed to facilitate remote electronic voting.

The requirements of the VVSG 2.x are more precise, more detailed, and written to be clearer to voting system manufacturers and test labs. Written in plain English, this document is usable by other audiences as well, including election officials, legislators, voting system procurement officials, various voting interest organizations and researchers, and the public at large.

The sub-paragraphs below describe the changes recommended to VVSG 2.x to support remote accessible ballot delivery, marking, return and storage. The recommendations are organized around each VVSG principle. Each principle has a corresponding set of test assertions that are used for system testing and certifications. The sub-paragraphs describe the changes that are needed to the test assertions in order to support electronic remote ballot delivery, marking, return, and storage.

3.1 High Quality-Design

The following requirements should be made to the High-Quality-Design Test Assertions:

The following test assertions do not apply to Remote Digital Ballot Delivery, Marking, and Return (RABDMR) because they relate to hand-marked ballot scanning or tabulation:

- 1.1.7-G – Scan to manufacturer specifications
- 1.1.7-H – Accurately detect imperfect marks
- 1.1.7-I – Ignore extraneous marks inside voting targets
- 1.1.7-J – Marginal marks, no bias
- 1.2-A – Assessment of accuracy
- 1.2-C – Minimum ballot positions

The following test assertions require modification:

- TA113A-1: Scanners and ballot marking devices MUST provide designated functions for entering voting mode

The following test assertions need to be added to the VVSG:

- **GBA-WG-1** - All marked ballots and related metadata shall be returned and recorded on a decentralized immutable ledger.

3.2 High Quality Implementation

The following test assertions do not apply to an RABDMR system:

- 2.1.1-C – Durability of paper

The following test assertions require modifications:

- **2.1.2-A –** Electronic device maintainability – 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.

- 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

The following test assertions need to be added to the VVSG:

- **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.

3.3 Transparent

The following test assertions do not apply:

- 3.1.2-B - Maximum tabulation rate
- 3.1.3-A - System Security
- 3.1.3-C - Physical Security
- 3.1.6-K - Marking Devices

The following test assertions require modification:

- 3.1.1-B – System overview, functional diagram – 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.
- 3.2-B – Minimum properties included in the setup inspection process
- 3.3-B – Specification of Common Data Format

The following test assertions need to be added to the VVSG:

- **GBA-WG-2** - The system shall have documented drawings and descriptions that illustrate adherence to applicable standards.

3.4 Interoperable

The following test assertions do not apply to an RABDMR system.

- **N/A**

The following test assertions require modification:

- **4.1-D – Exchange of voting device election event logs** - 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.
- **4.3-A – Standard device interfaces –** This only applies to vendor supplied hardware.

The following test assertions need to be added to the VVSG:

- **N/A**

3.5 Equivalent and Consistent Voter Access

The following test assertions do not apply to an RABDMR system.

- **N/A**

The following test assertions require modification:

- **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.

The following test assertions need to be added to the VVSG:

- **GBA-WG-3 -** The system shall authenticate eligible voters who are authorized to submit their ballot electronically.

3.6 Voter Privacy

The following test assertions do not apply to an RABDMR system.

- **6.1-D – Audio privacy**

The following test assertions require modification:

- **N/A**

The following test assertions need to be added to the VVSG:

- **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.
- **GBA-WG-5 -** The privacy of the marked ballot is maintained by the system.

3.7 Marked, Verified, and Cast as Intended

The following test assertions do not apply to an RABDMR system.

- 7.1-A – Reset to default settings
- 7.2-P – Floor space
- 7.2-R – Control labels visible

The following test assertions require modification:

- **7.1-N** – Tactile keys - These requirements seem to apply to vendor-supplied hardware.
- **7.2-A** – Display and interaction options - These requirements seem to apply to vendor-supplied hardware.
- **7.2-E** – Touch screen gestures – For remote voting, the election system vendor is responsible for supporting accessibility features that are native to the user's device.
- **7.3-K-16**: IF an alert is intended to confirm visual changes to the voter using an audio format THEN the voting system MAY communicate this with a short text OR sound. - Need To Be Discussed
- **7.3-M** – Identifying languages
- **7.3-O** – Instructions for election workers

The following test assertions need to be added to the VVSG:

- **GBA-WG-6 –** The voter shall be able to verify their marked ballot as cast.
- **GBA-WG-7 –** Prior to casting their ballot, only the eligible voter may mark or revise their ballot selection(s).
- **GBA-WG-8 –** The ballot cannot be cast by anyone other than an authenticated user.
- **GBA-WG-9 –** The system shall guarantee the recording of the ballot cast as marked.
- **GBA-WG-10 –** The system shall guarantee the ballot is recorded as cast.
- **GBA-WG-11 –** The system will ensure that only one marked ballot per eligible voter becomes a cast ballot.
- **GBA-WG-12 –** Vendors shall adhere to WCAG Version 2.1 level AA and provide the necessary VPAT documentation to prove adherence.

3.8 Robust, Safe, Usable, and Accessible

The following test assertions do not apply to an RABDMR system.

- **8.1-H – Sanitized headphones**

The following test assertions require modification:

- **TA83A-7:** Test participants MUST include blind voters using tactile controls. Unsure whether this means braille or could simply mean Voice-over, talkback and screen reader navigation. Needs clarification.
- **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.
- **TA83A-13:** The population under test SHOULD NOT consist of voters who have previously participated in a voting system usability test. Needs clarification.
- **TA83A-18:** The manufacturer SHOULD note any differences between the users profiled as recruits and the users who participated in the actual study.
- **TA83A-20:** The manufacturer SHOULD ensure that at least 30 test participants are able to complete the testing session. 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. 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. recommended, not mandatory
- **TA83A-26:** The test ballot used in the usability tests SHOULD look like a real ballot, such as the NIST test ballot.
- **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. Could "election worker" here refer to election official using admin console from their office?
- **TA84A-1-1:** The documentation SHOULD NOT presuppose familiarity with personal computers. Needs clarification.
- **TA84A-19:** The manufacturer MUST ensure that the election workers usability documentation/report is included in the TDP.

The following test assertions need to be added to the VVSG:

- N/A

3.9 Auditable

The following test assertions do not apply to an RABDMR system.

- **TA911A-1-1:** IF a voting system is a paper-based system THEN it MUST generate a paper record of votes cast.

The following test assertions require modification:

- **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.
- **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. To be considered for modification. More discussion needed.

The following test assertions need to be added to the VVSG:

- **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.

3.10 Ballot Secrecy

The following test assertions do not apply to an RABDMR system.

- **N/A**

The following test assertions require modification:

- **N/A**

The following test assertions need to be added to the VVSG:

- **GBA-WG-14** The system shall not be able to count ballots earlier than a moment in time specified by the jurisdiction.
- **GBA-WG-12** The immutable record shall be available in a human readable format at the appointed time.

3.11 Access Control

The following test assertions do not apply to an RABDMR system.

- **N/A**

The following test assertions require modification:

- **N/A**

The following test assertions need to be added to the VVSG:

- **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.

- **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.

3.12 Physical Security

The following test assertions do not apply to an RABDMR system.

- **TA121A-1:** The voting system MUST prevent access by chance OR access without intention.
- **TA121A-2:** The voting system MUST prevent opportunistic access. i.e., unauthorized access.
- **TA121A-3:** All unauthorized physical access attempts on the voting system SHOULD leave physical evidence.
- **TA121A-4:** All unauthorized access events that are successful MUST leave physical evidence.
- **TA121A-4-1:** IF unauthorized access occurs THEN the physical evidence MUST indicate the point of access
- **TA121A-5:** All physical access points on the voting system MUST be capable of being secured by tamper prevention methods (e.g., locks).
- **TA121A-6:** All physical access points on the voting system MUST be capable of being secured by tamper detection methods (e.g., seals, tape).
- **TA121A-7:** The voting system documentation MUST describe how to properly implement procedural and physical methods for detecting unauthorized access.
- **TA121B-1:** IF the *voter-facing* system component is in an activated stage AND IF the *voter-facing* system component is accessed in an unauthorized manner THEN the *voter-facing* system component MUST produce an alert
- **TA121B-2:** Alerts produced by the voting system MUST be EITHER audible OR visual in nature.
  TA121B-2-1: Audible alerts produced by the voting system SHOULD be greater than 60 dB.
- **TA121B-3:** Alerts MUST comply with requirements set forth in *7.3-K – Warnings, alerts, and instructions*.
- **TA121C-1:** IF a *voter-facing* system component is in an activated stage AND IF a component of a *voter-facing* system component is physically disconnected THEN the *voter-facing* system component MUST produce an alert.
- **TA121C-2:** Alerts produced by the voting system MUST be EITHER audible AND/OR visual in nature.
- **TA121C-3:** Alerts MUST comply with requirements set forth in *7.3-K – Warnings, alerts, and instructions*.
- **TA121D-1:** IF a *voter-facing* system component is in an activated stage AND IF *voter-facing* system component is physically *connected* THEN the *voter-facing* system component MUST log the *connection*.
- **TA121D-2:** IF a *voter-facing* system component is in an activated stage AND IF *voter-facing* system component is physically *disconnected* THEN the *voter-facing* system component MUST log the *disconnection*.
- **TA121E-1:** The manufacturer's documentation MUST specify tamper evident seals to be used for containers that *store* voting system records (e.g., ballots).
- **TA121E-2:** The manufacturer's documentation MUST specify tamper evident seals to be used for containers that *transport* voting system records (e.g., ballots).
- **TA121E-3:** The manufacturer's documentation MUST specify methods for properly applying seals on containers that *store* voting system records (e.g., ballots).

- **TA121E-4:** The manufacturer's documentation MUST specify methods for properly applying seals on containers that *transport* voting system records (e.g., ballots).
- **TA121E-5:** IF unauthorized physical access to a container *storing* voting system records occurs THEN the tamper evident seals MUST leave evidence of tampering when installed as documented.
- **TA121E-6:** IF unauthorized physical access to a container *transporting* voting system records occurs THEN the tamper evident seals MUST leave evidence of tampering when installed as documented.
- **TA121F-1:** IF the voting system uses locks THEN the voting system MUST be capable of supporting at a minimum, the following keying schemes:
- **TA121F-2:** Documentation MUST be provided by the manufacturer for each key scheme supported.
- **TA121G-1:** IF the voting system employs a physical security mechanism that requires power to operate, THEN that physical countermeasure MUST continue to operate using backup power if the power fails.
- **TA121G-2:** IF a voting system employs a powered physical security countermeasure, switching from primary power to backup power supply MUST produce an alert.
- **TA121G-3:** IF a power failure occurs for a physical security mechanism, THEN that physical countermeasure MUST automatically switch over to the backup power source.
- **TA121G-4:** IF the voting system employs a physical security mechanism that requires power to operate, THEN that physical countermeasure MUST generate an event log entry when the power fails.
- **TA122A-1:** Any *physical port* that is exposed MUST be essential to voting operations OR MUST be essential to testing the voting system OR MUST be essential to auditing the voting machine.
- **TA122A-2:** Any *access point* (e.g., panel, door) that is exposed MUST be essential to voting operations OR MUST be essential to testing the voting system OR MUST be essential to auditing the voting machine.
- **TA122B-1:** IF the voting system is in an *activated* stage, THEN the voting system MUST automatically disable any digital communication *port* that is disconnected.
- **TA122B-2:** IF the voting system is in a *suspended* stage, THEN the voting system MUST automatically disable any digital communication *port* that is disconnected.

The following test assertions require modification:

- **N/A**

The following test assertions need to be added to the VVSG:

- **N/A**

3.13 Data Protection

The following test assertions do not apply to an RABDMR system.

- **N/A**

The following test assertions require modification:

- **N/A**

The following test assertions need to be added to the VVSG:

- **N/A**

3.14 System Integrity

The following test assertions do not apply to an RABDMR system.

- **TA142C-1:** The voting system MUST NOT establish wireless connections.
- **TA142C-2:** The voting system MUST NOT broadcast or advertise a wireless network.
- **TA142C-3:** The voting system MUST NOT accept connection requests.
- **TA142C-4:** The voting system MUST disable any wireless functionality by default.
- **TA142D-1:** IF a voting system contains wireless functionality, THEN there MUST always be a status indicator confirming that wireless networking functionality is disabled.
- **TA142E-1:** IF a voting system can establish a connection to an external network THEN the voting system MUST NOT allow any wireless OR any wired connection to a network.
- **TA142E-2:** All voting system components MUST utilize non-routable IP addresses.
- **TA142E-3:** IF a voting system can establish a connection to an external network THEN the voting system MUST NOT allow any device external to the voting system to connect to that network.
- **TA142J-1:** The voting system MUST NOT bulk import OR include libraries that the voting application does not need to function.

The following test assertions require modification:

- **N/A**

The following test assertions need to be added to the VVSG:

- **GBA-WG-19** The system shall meet a minimum error rate in accordance with the VVSG accuracy requirement.

3.15 Detection and Monitoring

The following test assertions do not apply to an RABDMR system.

- **TA154C-1:** The voting system documentation MUST include instructions for physically removing power from any embedded wireless chipsets.
- **TA154D-1:** The voting system MUST be capable of *updating* rules and policies to *network appliances*.
- **TA154D-2:** The voting system MUST be capable of *utilizing* updated rules and policies for *network appliances*

The following test assertions require modification:

- **N/A**

The following test assertions need to be added to the VVSG:

- **N/A**

3.16 Communications

The following test assertions do not apply to an RABDMR system.

- **N/A**

The following test assertions require modification:

- **N/A**

The following test assertions need to be added to the VVSG:

- **GBA-WG-20** Until the ballot is submitted, no marked ballot data is transmitted.
- **GBA-WG-21** The correct ballot is delivered to (and only to) the eligible voter.
- **GBA-WG-22** The marked ballot is returned from only the voter who received the ballot.
- **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.
- **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]

4 Conclusions & Recommendations

4.1 Conclusion

With the requirement for LEOs to support voting by overseas and disabled voters, remote voting methods and systems are absolutely required. There are programs in place to test and certify systems for the delivery, marking, return of paper ballots. However, there are other electronic methods of remote voting in use including:

- Faxed ballots
- Email
- File uploads
- Browser based digital ballots &
- Application based digital ballots

The Election Assistance Commission (EAC) will need to support the full spectrum of voting technologies, methods, and systems. The analysis of the VVSG from the perspective of remote ballot delivery, marking, and return is just the first step in evolving the VVSG into a standard that is sufficient for the many options and choices have today.

4.2 Recommendations

The Voluntary Voters System Guidelines (VVSG) will need to be modified in order to support remote accessible ballot delivery, marking, and return (RABDMR). The Government Blockchain Association (GBA) Voting Working Group has identified several test assertions that will require modification. The authors of this study recommend that the EAC review this report and incorporate the appropriate changes in the next version of the VVSG. The members of this working group stand ready to support the EAC in the continuous improvement efforts to adapt current election standards to reflect the increasing capabilities and implementations of secure digital communications. Consequently, the members of the Government Blockchain Association Voting Standards Working Group recommend that the EAC convenes a group to review the findings in this report and implement the ones that support the mission and goals of the EAC.

End Notes

[i] www.history.com/news/vote-by-mail-soldiers-war

[ii] www.eac.gov/sites/default/files/eac_assets/1/28/William-Kelleher-Internet-Voting-WPSA-Paper-July-9th.pdf https://www.eac.gov/sites/default/files/TestingCertification/Voluntary_Voting_System_Guidelines_Version_2_0.pdf