Government Blockchain Association
Remote Election Technology Report

July 29, 2022

Final

This report is the product of the

Government Blockchain Association
10560 Main Street, Suite 608
Fairfax, Virginia, 20030
www.GBAglobal.org

It is intended to be informative and for public consumption.

Acknowledgements

On March 4, 2021, the Government Blockchain Association (GBA) hosted an event called Blockchain & Voting. During that event it became crystal clear that there were several opposing perspectives concerning remote accessible digital ballots, markings, and returns. A vigorous debate arose regarding the pros and cons of remote digital voting methods compared with other remote voting methods.

The full debate can be viewed by clicking the image to the left.

Following the debate, the GBA invited all members of the discussion to collaboratively perform an apples-to-apples comparison of various remote voting return methods.

After over a year of working together, the participants gathered to draft, review, and finalize their findings. Additional experts, not part of the original panel, also joined the discussion. Together, the community produced the following report.

The GBA would like to extend a heartfelt thanks to all the professionals who labored diligently over the past year to produce this document. Our hope is that it educates and inspires elections officials to select technologies that meet the needs of their constituents.

Sincerely,

Gerard R. Dache

Gerard R. Dache
Executive Director
Government Blockchain Association

Table of Contents

1 Introduction 1
1.1 Purpose 1
1.2 Study Methodology 1
1.3 Report Structure & Content 2
1.5 Key Concepts, Notes & Assumptions 3
1.5.1 Accessibility 3
1.5.2 Ballot Integrity Confidence 3
1.5.3 Chain of Control 3
1.5.4 Chain of Custody 3
1.5.5 Voter Privacy 3
1.5.6 Notes, Clarifications, & Assumptions 4
2 Remote Ballot Return Methods 5
2.1 Official mailed paper ballot & envelope 6
2.2 Voter-printed ballot & envelope 6
2.3 Simple fax ballot return 7
2.4 Simple email ballot return 7
2.5 Simple file upload ballot return 8
2.6 Browser based, digitally protected ballot return 8
2.7 App based, digitally protected & ledgered ballot return 10
3 Functional Points of Comparison 11
3.1 Accessibility (Voter) 11
3.2 Usability (Voter) 11
3.3 Interoperability (Election Administration) 11
3.4 Convenience (Voter) 11
3.5 Resilience 12
3.6 Transparency 12
3.7 Ballot Secrecy 12
4 Comparison of Remote Ballot Return Methods 13
4.1 Functional Comparison Matrix 13
5 Security Points of Comparison for Remote Ballot Return 15
5.1 Tamper Evident 16

5.2 Destruction Evident 16
5.3 Digital Data Privacy, Security, and Integrity Protection 16
5.4 Preserves Voter Privacy via Permanent Separability 16
5.5 Post-Election Audit of Voters' Original Ballots 17
5.6 Human Ballot Physical Proximity Required for Tampering 17
5.7 Group-Limited Threat Actor Scale 17
6 Security Comparison Matrix 18
Appendix A: Glossary 1
Appendix B: Endnotes for Security Points of Comparison 1

1 Introduction

1.1 Purpose

Elections are one of the most important public sector processes performed by democratic societies. Consequently, changes to time-honored elections processes are approached with extreme caution and careful consideration. At the same time, changes in technology and other factors have resulted in numerous proposals to election processes, procedures, tools, and technologies. One of the most significant changes being considered is the use of remote voting using electronic methods. In the 2018 and 2020 US General Election, multiple states took advantage of emerging internet technologies to offer overseas citizens, members of the military, and voters with disabilities a means of voting remotely. However, state and local election officials have expressed concern about the lack of standards and certification processes.

Currently, there is significant debate about the security and relative advantages/disadvantages of remote ballot delivery, marking, return, and storage. Local Election Officials (LEOs) are expected to consider, evaluate, and select solutions that may involve remote electronic voting systems. Various organizations such as the Open-Source Election Technology (OSET) Institute, the Verified Voting Foundation, vendors, as well as other academic institutions, and other associations have worked diligently to help educate lawmakers, policy makers, and election officials about the features, benefits, and risks of these methods.

On March 4, 2021, several elections experts representing a diverse set of opinions were invited by the Government Blockchain Association (GBA) to engage in a public discussion on the topic of Blockchain & Voting. The expert panel included:

- An election official
- A vendor of remote voting systems
- US and European industry associations
- Academic professionals
- A blockchain community representative

The discussion revealed that opposing views may result from an inappropriate comparison of the methods, and that performing an objective comparison would be beneficial to evaluating the security and appropriateness of various methods of remote ballot return. The discussion participants agreed that it would be beneficial to perform an analysis of the various methods and make the resulting information available to election officials and the wider community.

This report is the result of months of study, analysis, and collaboration between industry experts to support election officials in their comparison of remote ballot return methods.

1.2 Study Methodology

The study group's first activity was to establish a charter. The charter defined the scope, participants, major activities, communication protocols and mutually established expectations. Individual members drafted the content of the report in a shared repository. The group met each week over the course of approximately nine months to draft this report.

The group identified seven methods of returning the marked ballot from a remote location. The criterion for evaluation was that the method was used in a recent election and included returning the marked ballot by post, email, fax, or via the internet. The study compares the various methods of ballot return based on an agreed list of functional and security points of comparison.

Once the report was drafted, it was circulated to a wider community of elections officials and related stakeholders for review and comment. Those comments were reviewed and incorporated into the study. The finalized report was released to each member of the study group.[1]

1.3 Report Structure & Content

This document provides legislators, election officials, voters, and other stakeholders with a balanced analysis of the capabilities, security, and risks of the currently available Remote Ballot Return Methods. The report compares the functionality and security of remote ballot methods in the following structure:

- Section 1 describes the motivation, methodology, and output of the **study**.
- Section 2 describes the seven methods of remote ballot return with **workflow diagrams**.
- Section 3 describes the key **functional characteristics of comparison**.
- Section 4 presents the **functionality matrix** comparing the identified Methods of Remote Ballot Return.
- Section 5 describes the key **security characteristics of comparison**.
- Section 6 presents the **security matrix** comparing the identified Methods of Remote Ballot Return (followed by endnotes.)
- Appendix A is a **Glossary** of terms

The goal of this report is to support the Local Election Official (LEO) in understanding the risks and benefits associated with the various methods of return to inform their decisions.

[1] This statement will be true once the study is complete. However, it is a forward-looking statement until the document is distributed for review, comment, and update.

1.5 Key Concepts, Notes & Assumptions

The following sections describe concepts and clarifications that are used throughout the report.

1.5.1 Accessibility

Accessibility refers to characteristics that make a system available and usable by voters with disabilities. Common disabilities are vision, hearing, mobility, cognitive and dexterity impairments.

1.5.2 Ballot Integrity Confidence

The term **ballot integrity** refers to the assurance that a remote ballot is not modified or deleted. A ballot is **verified** if it is approved for tabulation via the **remote ballot verification process** in which LEOs approve or reject a ballot for future counting, based on multiple procedures that include checking the affidavit for a match with voter registration records; matching the affidavit signature to a signature on file; checking whether the voter has already voted in the current election, or has otherwise become ineligible. as well as other means.

1.5.3 Chain of Control

Chain of Control refers to the ballot after it leaves the control of the LEO to the voter, up to the point where the marked ballot is returned to the custody of election officials. This may include several modes of transport. For the purposes of comparing return methods, this report focuses on threats to the ***chain of control*** during the process of transporting a remote ballot and affidavit from a voter to LEO.

Return methods differ significantly in the details and security of this latter chain of control, with a ballot passing through the undocumented control of several different modes of transit (e.g., postal facilities, email, and file servers).

1.5.4 Chain of Custody

The **Chain of Custody** of a marked ballot begins once the LEO has accepted the ballot and ends at the end of the statutory retention period. Chain of Custody refers to the processes, or paper trail, that documents the transfer of materials from one person (or place) to the next in possession of local election officials.

Every state and local jurisdiction has its own controls for ensuring that the chain of custody of election materials is properly maintained. These controls may include physical and digital safeguards including locks, seals, audit logs, witness signatures, physical & digital controls on servers storing ballots and affidavits.

For this technology report, the term custody refers to the presence of the marked ballot on the physical premise of, or on the computing resources supporting the election office.

1.5.5 Voter Privacy

Voter privacy is the ability to cast a ballot without revealing their ballot selections to anyone else

1.5.6 Notes, Clarifications, & Assumptions

The following are notes, clarifications, and assumptions that were agreed upon by the members of the study group.

- The comparisons only involved the return of a marked ballot. Different return methods and different vendors may require different identity verification methods for a voter to receive a ballot. Some return methods and vendors may require identity verification with official photo identification, biometrics, or a PIN, for example. Identity verification requirements for ballot receipt were not compared in the security comparison since they were out of scope of ballot return.
- This study is not restricted by current legislation since laws can be changed. The analysis was constrained by the capabilities of current implementations.
- There are three main stages of remote ballot delivery, marking, and return:
    1. The LEO delivers the ballot to the voter,
    2. The voter returns the marked ballot to the LEO, and
    3. The LEO receives, accepts & maintains possession of the ballot.
- Security of ballot return necessarily has two facets: accepting and maintaining the integrity of a legally cast ballot and rejecting ineligible and illegal ballots. A returned ballot is **cast legally** if
    1. The marked ballot reflects the intent of the individual to whom the ballot was sent by the LEO
    2. That individual is alive and resides in the jurisdiction (or, in the case of an overseas voter, most recently resided in that jurisdiction) corresponding with the returned ballot
    3. That individual is registered in that jurisdiction, and
    4. Is eligible to be registered (e.g., is a U.S. citizen and is at least 18 years old).

  This definition encompasses the need for some voters to have a trusted family member or aide to mark and return a ballot on the voter's behalf; this action reflects the intent and approval of the voter. By contrast, examples of ballots **cast illegally** include:

    1. a ballot delivered to a deceased voter that has been marked and returned with a forged signature on the affidavit; or
    2. a ballot marked and returned against the knowledge and/or will of the voter to whom the ballot was addressed, with a forged signature on the accompanying affidavit.

  These examples are certainly not exhaustive and would be difficult for a LEO to identify as fraudulent if the signature forgery was of sufficient quality.

- Considering the above, the study participants assume that the LEO is in the best position to determine whether a received ballot is eligible or not and that the voter registration records used to determine this eligibility are properly maintained and have no voters on the rolls that are fabricated, deceased, have moved to another jurisdiction, are no longer U.S. citizens, or are otherwise ineligible to vote.

- The study participants acknowledge that some return methods and some vendors may allow for and include authentication (not to be confused with identification) methods beyond affidavit signatures, including a cryptographic digital signature or unique ballot identification number, that could be used in the absentee ballot verification process.

2 Remote Ballot Return Methods.

All US jurisdictions offer some form of remote ballot return. Traditionally, this is an official mailed paper ballot. However, these ballots are not accessible to many voters including those with visual or dexterity disabilities. In addition, they are often impractical for citizens serving, working, or studying abroad. Further, all voters can be impacted by hurricanes, pandemics, and other disasters.

The needs of these citizens have prompted legislation such as HAVA[2], UOCAVA[3] and led to development of alternate remote voting solutions. In fact, at least seven distinct methods of remote ballot return now address the needs of overseas and disabled voters in the US. Now all of them afford the local election office (LEO) methods of ensuring every eligible citizen the ability to return their marked ballot and have their vote included in the final tally. However, these remote ballots return methods differ in security and functionality. They are:

- 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

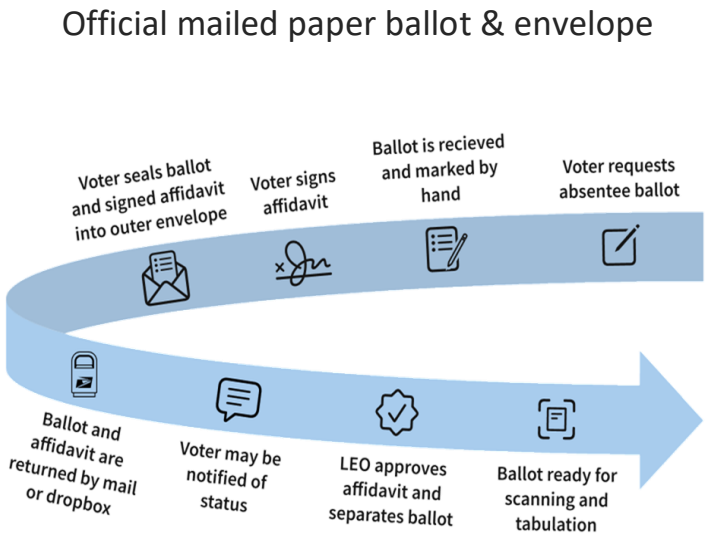
To compare the various methods of remote ballot return, it is necessary to first provide descriptions and workflows of the seven methods of return. The following section describes each of the methods evaluated in this report.

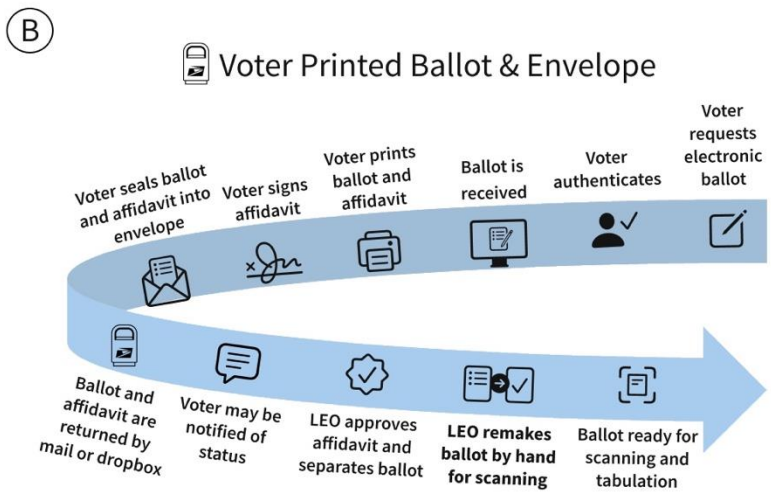
Each workflow diagram begins with the voter obtaining the ballot, marking the ballot, and preparing the ballot and affidavit package for return. The workflow then continues to identify the steps required for the LEO to review the ballot package and to prepare the ballot for tabulation.

Note: A key element of remote ballot return is determining the voter's eligibility to cast their ballot using one of the seven described remote ballot return methods. The method of voter identity verification is out of scope of this document. The various methods of authenticating the eligible voter submitting their marked ballot is via a means of authentication that the registered user is submitting the ballot.

[2] Help America Vote Act (HAVA)
[3] Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA)

2.1 Official mailed paper ballot & envelope	2.2 Voter-printed ballot & envelope
This method includes the following sequence of steps: 1. Voter requests official mailed paper ballot 2. Ballot is received and voter hand marks 3. Voter inserts marked ballot into inner envelope 4. Voter signs affidavit and inserts with inner envelope in the outer envelope. 5. Voter returns envelope via postal mail or authorized dropbox. 6. Voters may obtain confirmation of receipt and/or review status. 7. LEO approves affidavit then separates from paper ballot 8. Ballot ready for optical scanning & tabulation.	This method includes the following sequence of steps: 1. Voter requests electronic ballot delivery. 2. Voter verification authenticates based on LEO's requirements 3. Ballot is received electronically. 4. Voter marks ballot electronically and prints ballot, affidavit, and envelope, (*OR* prints ballot first and marks by hand.) 5. Voter signs affidavit and constructs envelope. 6. Voter inserts ballot and affidavit in envelope 7. Voter returns envelope via postal mail or authorized dropbox. 8. Voters may obtain confirmation of receipt and/or review status. 9. LEO approves affidavit and separates from paper ballot. 10. LEO remakes ballot for optical scanning. 11. Ballot ready for optical scanning & tabulation.





2.3 Simple fax ballot return

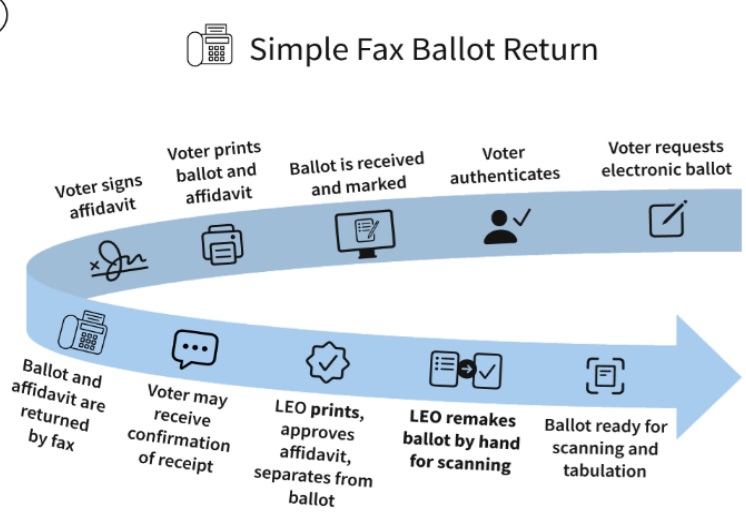
1. *Voter requests access for digital return of hand marked or electronic ballot*
2. Voter verification based on LEO's requirements
3. Ballot is received electronically.
4. Voter receives and marks ballot electronically and prints ballot, affidavit, and envelope, OR b. Voter prints the ballot, affidavit, envelope and marks by hand.
5. Voter signs affidavit.
6. Voter faxes (physical or efax) to Jurisdiction with confirmation of delivery.
7. LEO approves affidavit and separates from ballot.
8. LEO prints ballot and remakes ballot by hand for optical scanning.

2.4 Simple email ballot return

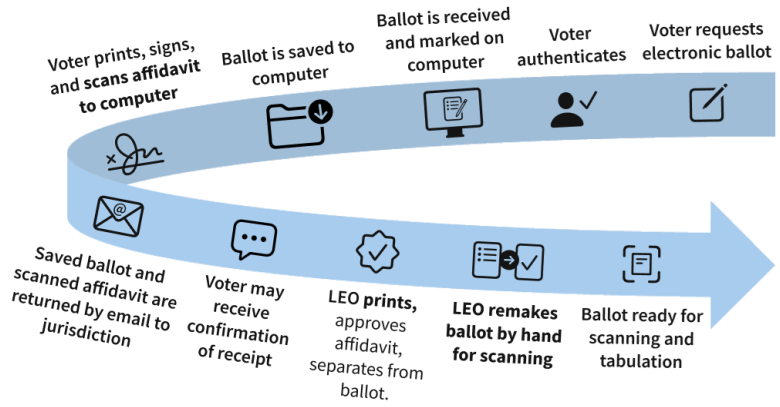
1. *Voter requests access for digital return of hand marked or electronic ballot*
2. Voter verification based on LEO's requirements
3. Ballot is received electronically.
4. Voter receives and marks ballot electronically and prints ballot, affidavit, and envelope, OR b. Voter prints ballot, affidavit, envelope and marks by hand.
5. Voter prints, signs and scans affidavit to computer.
6. Voter attaches documents and returns via ordinary email.
7. *Voters may obtain confirmation of receipt and/or review status.*
8. LEO approves affidavit and separates from ballot.
9. LEO prints ballot and remakes ballot by hand for optical scanning.
10. Ballot ready for optical scanning & tabulation.

9. Ballot ready for optical scanning & tabulation.

C



D



2.5 Simple file upload ballot return

1. *Voter requests access for digital return of hand marked or electronic ballot*
2. Voter verifies identity and receives ballot electronically.
3. Voter marks the ballot electronically and saves it to the computer (or prints and marks by hand.)
4. Voter prints, signs, and scans affidavit to computer.
5. Voter authenticates (logs in) based on LEO's requirements
6. Voter uploads documents to web portal.
7. *Voters may obtain confirmation of receipt and/or review status.*

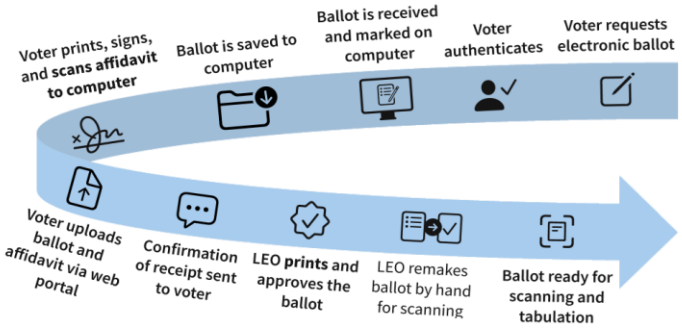
2.6 Browser based, digitally protected ballot return

1. *Voter requests electronic ballot.*
2. LEO sends invitation to vote.
3. Voter verifies identity based on LEO's requirements
4. Voter receives and electronically marks the ballot.
5. Voter electronically signs affidavit. *(See note below.)*
6. Ballot and affidavit are cryptographically protected and transmitted via electronic networks to Jurisdiction
7. Voter receives a confirmation of receipt of submission
8. LEO approves affidavit which enables viewing of ballot
9. Jurisdiction remakes ballot for optical scanning.

8. LEO approves affidavit and separates from ballot.
9. LEO prints ballot and remakes ballot by hand for optical scanning.
10. Ballot ready for optical scanning & tabulation.

(E)

Simple File Upload Ballot Return

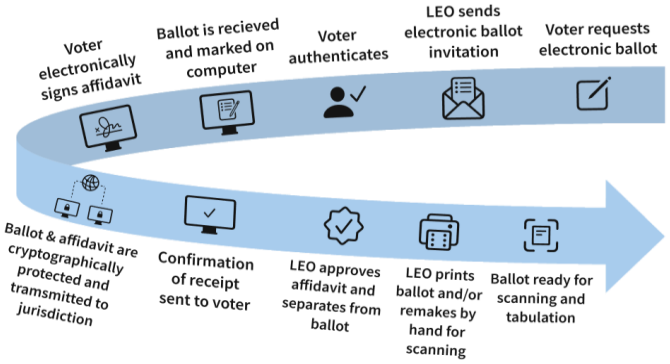


10. Ballot ready for optical scanning & tabulation.

Note: This method of return permits supplemental or alternative advanced authentication techniques.

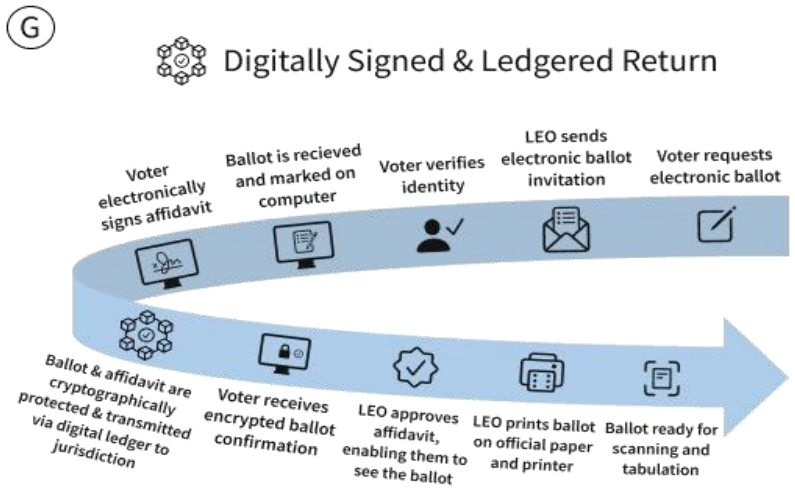
(F)

Digitally Protected File Upload Return



2.7 App based, digitally protected & ledgered ballot return

1. *Voter requests electronic ballot.*
2. LEO sends electronic ballot invitation.
3. Voter verifies their identity based on LEO's requirements.
4. Voter receives and electronically marks the ballot.
5. Voter authenticates by electronically signing affidavit. *(See note below.)*
6. Cryptographically protected ballot & affidavit are transmitted to and recorded on the jurisdiction's secure digital ledger.
7. Voter receives a confirmation of receipt of submission (*Voter may receive enhanced encrypted ballot confirmation.)*
8. LEO approves affidavit which enables viewing ballot
9. LEO prints ballot on official paper/printer
10. Ballot ready for optical scanning & tabulation.



3 Functional Points of Comparison

These following criteria were used to evaluate statutory, usability or integration functionality of the various seven remote ballot return methods.

3.1 Accessibility (Voter)

Accessibility refers to characteristics that make a system available and **usable by voters with disabilities**. Common disabilities are vision, hearing, mobility, cognitive and dexterity impairments. Traditional paper ballots are not considered accessible.

- Accessibility includes **measurable compliance with current standards** such as Web Content Accessibility Guidelines (WCAG) and Voluntary Voting System Guidelines (VVSG).
- It may also include support for **assistive technologies** such as screen readers, and input devices and/or changes in format to accommodate disabilities (e.g., large fonts).
- This includes using one's own assistive technologies.

3.2 Usability (Voter)

Usability in the context of voting refers to voters being able to **cast valid votes as they intended quickly, without errors**, and with confidence that their contest and question selections were recorded correctly.

- VVSG specifies Usability criteria for both electronic ballot design, including checks to prevent accidentally over-voting/under-voting ballots, and to allow for entering write-ins.
- Voters can navigate, review and change selections easily without needing assistance by officials.
- Voters can request/view their ballot in native language if supported by the jurisdiction.

3.3 Interoperability (Election Administration)

Interoperability refers to the **ease of which electronically marked ballots interface with other channels of voting permitted by the jurisdiction** in overall election processes. Examples are:

- Directly reading the ballot data and styles from Election Management System (EMS).
- Integration with voter lists/poll books to verify voter eligibility.
- The marked paper ballot is a representation of the digital ballot.
- Minimizes the likelihood that election officials need to 'remake' the voter's ballot onto another physical ballot format for tabulation.
- Permits Logic & Accuracy testing with appropriate audit logging.

3.4 Convenience (Voter)

A convenient system **avoids voters needing assistance or accommodation to cast their ballot securely, and on time, without compromising their privacy.** Considerations may include transportation and voting window dates.

Convenience also involves voter's access to required equipment (e.g., fax machine, printer, mobile device, etc.)

3.5 Resilience

Resilience is defined as an organization's **ability to maintain acceptable service levels through, and beyond, severe disruptions to its critical processes and systems** by means of redundancy **included in the business continuity plan.** It also means reducing the risk of system failure, e.g., removing single points of failure.

- The method of return is capable of withstanding a disruption and guarantees the timely delivery of the marked ballot to the LEO.
- The method of return can be adapted to conform to continuity operations in the case of natural or other disasters.
- There are no time bound constraints that would interfere with the voters' ability to submit their intent from any secured network.

3.6 Transparency

A remote voting method is **transparent** if a voter or auditor can determine that a ballot was received by the LEO, and it provides clear **chain of custody.**

- Enables a voter to receive confirmation, which could include reviewing LEO website or receiving text, email, or other notification of receipt.
- This confirmation may include notice that the marked ballot was (a) sent or (b) received or (c) received & ready for tabulation.
- A transparent open process permits independent observation of process by staff, stakeholders, and political parties.
- Supports post-election audits supported by the LEO that allow for observation.

3.7 Ballot Secrecy

The voting system is designed and deployed to ensure voters can mark, verify, and cast it without revealing their ballot selections. The system demonstrates that voter verifiability and voter anonymity are both ensured. A goal of voting systems is to ensure that no contest selections can be associated with a voter.

Typically ballot secrecy is achieved by separating the marked ballot from voter identity and assuring that the marked ballot and the voter's identity cannot be reconnected.

4 Comparison of Remote Ballot Return Methods

4.1 Functional Comparison Matrix

Functional Points of Comparison							
Method of Return of Marked Ballot	**Official Paper Ballot Return (a)**	**Voter Printed Ballot Return (b)**	**Fax Ballot Return (c)**	**Email Ballot Return (d)**	**Simple File Upload Ballot Return (e)**	**Browser Based Digitally Protected File Upload Ballot Return (f)**	**App Based, Digitally Protected & Ledgered Return (g)**
Accessibility (Voter)	Medium	Low	Low	Low	Medium	High	High
Usability (Voter)	Low	Low	Low	Low	Low	High	High
Interoperability (LEO)	High	Low	Low	Low	Medium	High	High
Convenience (Voter)	Medium	Low	Low	Medium	Medium	High	High
Resilience	Low	Low	Low	Low	Low	Medium	Medium
Transparency (Voter)[4]	Medium	Low	Low	Low	Medium	Medium	High
Ballot Secrecy	High	Low	Low	Low	Low	Medium	High

[4] Provides a grounded chain of custody for post-election audit.

5 Security Points of Comparison for Remote Ballot Return

The goal of this section is to compare security properties of various methods of remote ballot return. Security properties can be neatly divided into two main categories:

- **ballot integrity**
- **voter privacy (i.e. ballot anonymity).**

Both ballot integrity and voter privacy risk compromise during two distinct types of 'chain of custody'. One type consists of physical and procedural controls implemented by election officials' staff to maintain documented access control over remote ballots once the ballots have arrived in their custody. The other type might be better referred to as the 'chain of control' of a ballot after it leaves the control of the voter, up to the point where the ballot is in the custody of election officials. Return methods differ significantly in the details and security of this latter chain of control, with a ballot passing through the undocumented control of several different modes of transit (e.g., postal facilities, email, and file servers).

(1) **Transport Chain of Control** is the period when an election official can have level of confidence in the security of the method of return of the marked ballot as compared with the service of the United States Post Office.

(2) **LEO's Chain of Custody** of a marked ballot begins once the LEO receives the ballot and ends at the end of the statutory retention period.

This section uses the term **Threat Actor** in reference to a nation state, a ballot trafficking syndicate, criminals, hackers, compromised insiders, or other parties attempting to interfere in the return of the marked ballot. A threat actor attempts to compromise an election. This section attempts to assess the risks associated with various return methods.

LEOs face a potentially wide scope of threat actors who can attempt to compromise the anonymity of ballots and the integrity of ballots and affidavits. There are different ways that a digital ballot return method can affect that scope. A return method can have a wide range of threat actors to ballots and affidavits en route, that is, threat actors that do not need specialized skills or resources. A return method can have a narrow range of threat actors, that is threat actors that need special skills, resources, or insider access. Some digital return methods have a *potentially* narrow scope of threat actors as a result of cryptographic protections that limit the scope to threat actors who can obtain the cryptographic keys needed to undo the protections. That scope is narrow only if the cryptographic protections are properly applied and properly managed by LEOs; if not, there is a wider scope of digital threat actors to ballots and affidavits both in route and after arrival to digital storage. The following points of comparison consider these attack scopes.

The seven security points of comparison are described below.

5.1 Tamper Evident

A ballot is **tamper evident** if an attack that changes, modifies, or replaces data on a remote ballot or voter affidavit can be reliably detected by LEOs.

Values: **Yes / No**

5.2 Destruction Evident

A ballot is **destruction evident,** if LEOs can reliably detect an attack that destroys a remote ballot and affidavit.

Values: **Yes / No**

5.3 Digital Data Privacy, Security, and Integrity Protection

An electronically returned ballot and affidavit have **digital data security** if currently standard encryption and data integrity techniques are used to protect personally identifying information (PII), the affidavit, and ballot data on a marked and cast ballot within the chain of control of the ballot. This requires the following:

- Standard encryption methods and sufficiently strong keys.
- Cryptographic measures to protect data integrity.
- Robust anti-malware protection on a voter's device, LEO computers and servers, and vendor servers.
- Real-time data anomaly detection on a voter's device, LEO computers and servers, and vendor servers.
- Protection against side-channel attacks.
- Robust protection against denial-of-service attacks on servers.

Additionally, these methods can be used for digital authentication of the ballot.

Values: **Yes / No**

5.4 Preserves Voter Privacy via Permanent Separability

The **preserves voter via permanent separability** point of comparison describes whether a return method includes the ability to perform privacy-masking of a remote ballot with voter affidavit, so that the ballot and affidavit are not simultaneously visible, thus providing a protection of voter privacy. In some cases, a return method does not enable voter privacy while the remote ballot with voter affidavit is in transit, but LEOs can optionally choose to anonymize the ballot material once it is in the custody of the LEO, for example, by printing an emailed ballot and affidavit, and putting the ballot in a privacy sleeve.

It also describes whether a return method supports the ability to perform a permanent separation of ballot from affidavit, e.g., physically separating one voter's one ballot from its accompanying affidavit, with mixing that prevents the re-association of that one affidavit with that one ballot, thus providing a protection of voter privacy.

Values: **Yes / No**

5.5 Post-Election Audit of Voters' Original Ballots

The **post-election audit of voter's original ballot** point of comparison describes whether, for ballots returned via a given return method, the ballots used for tabulation, and a post-election ballot audit were originally marked by the voter. Ballots transcribed by the LEO for optical scanning require auditing both the voter's and remade ballots.

Values: **Yes / No**

5.6 Human Ballot Physical Proximity Required for Tampering

This point of comparison describes whether LEOs face threat actors that are limited to local attacks requiring physical proximity to remote ballots with voter affidavit. By contrast, an attack could include a potentially global set of threat actors who can attack ballot integrity and ballot anonymity from a remote location.

Values: **Yes / No**
Yes means that attacks are limited to local actors. **No** means attacks include those with global reach.

5.7 Group-Limited Threat Actor Scale

The **group-limited threat actor scale** point of comparison describes whether threat actors are limited in access to single ballots or groups of ballots in a single attack, or whether a single attack can cause wholesale destruction, tampering, or anonymity violations affecting all or a large portion of ballots. In practice, a scale of single ballots only applies to postal return, and only part of the time, so single-ballot scale is not noted.

Values: **Yes / No**
Yes means limited to a group attack; **No** means includes the threat of wholesale attacks.

6 Security Comparison Matrix

Security Points of Comparison							
Method of Return of Marked Ballot	**Official Paper Ballot Return (a)**	**Voter Printed Ballot Return (b)**	**Fax Ballot Return (c)**	**Email Ballot Return (d)**	**Simple File Upload Ballot Return (e)**	**Browser Based Digitally Protected File Upload Ballot Return (f)**	**App Based, Digitally Protected & Ledgered Return (g)**
Tamper Evident	No	No	No	No	No	Yes	Yes
Destruction Evident	No	No	No	No	No	No	Yes[i]
Digital Data Security & Integrity Protection	N/A	N/A	No	No	No	Yes	Yes
Preserves Voter Privacy via Permanent Separability	* [ii]	* [iii]	No	No	No	No	* [iv]
Post-Election Audit of Voters' Original Ballots	Yes	Yes[v]	No	No	No	No	No
Human Ballot Physical Proximity Required for Tampering	Yes	Yes	No	No	No	No	No [vi]
Group-limited Threat Actor Scale	* [vii]	Yes [viii]	No	No	No	No	* [ix]

The Endnotes and asterisks indicate where the authors did not reach consensus on one of the security table's comparators. There are a variety of remote election systems in use so it is challenging to generalize. Additional discussion is provided in endnotes in Appendix B.

Appendix A: Glossary

Appendix A: Glossary

Obtained from US Election Assistance Commission (EAC.GOV) or National Institute of Standards and Technology (NIST.GOV), unless otherwise noted.

- EAC: www.eac.gov/sites/default/files/TestingCertification/Voluntary_Voting_System_Guidelines_Version_2_0.pdf
- NIST: https://pages.nist.gov/ElectionGlossary

Term	Definition	Source
Adjudication	Process of resolving flagged cast ballots to reflect voter intent. Common reasons for flagging include: ● write-ins, ● overvotes, ● marginal machine-readable mark, ● having no contest selections marked on the entire ballot, or ● the ballot being unreadable by a scanner.	NIST.GOV and EAC.GOV
Audit	1. Systematic, independent, documented process for obtaining **records**, statements of fact, or other relevant information and assessing them objectively to determine the extent to which specified requirements are fulfilled. 2. Verification of statistical or exact agreement of records from different processes or subsystems of a **voting system**. 3. A review of a system and its controls to determine its operational status and the accuracy of its outputs.	EAC.GOV
Authentication	Verifying the identity of a user, process, or **device**, often as a prerequisite to allowing access to resources in an information system.	EAC.GOV

Appendix A: Glossary

Cast Ballot (noun)	Ballot in which the voter has taken final action in selecting contest options and irrevocably confirmed their intent to vote as selected. Synonyms: voted ballot *(Note: for purposes of remote return, is this submitting the ballot for delivery to local election office, regardless of method?)*	NIST.GOV and EAC.GOV
Digital Signature	A cryptographic operation where a **private key** is used to digitally sign an electronic document and the associated **public key** is used to verify the signature. Digital signatures provide data **authentication** and integrity protection.	EAC.GOV
Election Management System (EMS)	Set of processing functions and databases within a **voting system** typically used to: ● develop and maintain **election definition** data, ● perform **ballot** layout functions, ● create ballot presentation templates for ballot printers or **devices** used by **voters** for ballot markup, ● **tabulate votes**, ● consolidate and **report** results, and ● maintain **audit trails**. Synonyms: EMS	EAC.GOV
Marked Ballot	**Ballot** that contains all of the selections made by a **voter** (see also manually-marked paper ballot)	EAC.GOV
Privacy (for voters)	A property of a **voting system** that is designed and deployed to enable **voters** to obtain a **ballot**, and mark, verify, and **cast** it without revealing their ballot selections or selections of language, display and **interaction modes** to anyone else. This does not preclude the ability of a voter to request assistance under state	EAC.GOV

Appendix A: Glossary

	law. Also: **ballot secrecy** A goal of **voting systems** to ensure that no **contest selections** can be associated with a **voter**.	
Recorded Ballot	A ballot for which there is an associated **cast vote record**	EAC.GOV
Threat Actor	A threat actor is any individual or group of individuals who attempt to interfere in the return of a marked ballot or compromise an election. For example, a threat actor may be a nation state, ballot trafficking syndicate, criminal, hackers, compromised insider, or other party.	Remote Election Working Group
Voter Affidavit	Jurisdiction-specific document accompanying marked ballot attesting the voter's eligibility to vote. Text varies by jurisdiction and may also waive privacy rights for certain return methods (e.g. marked ballot return by email, etc.)	Remote Election Working Group

Appendix B: Endnotes for Security Points of Comparison

Appendix B: Endnotes for Security Points of Comparison

The endnotes indicate where the authors did not reach consensus on one of the Security table's comparators. There are a variety of remote election systems in use so it was challenging to generalize in each of the generic ballot return categories below.

Further, this document's scope is to compare remote return methods while under election officials' custody/visibility. (This excludes delivery means outside of their control such as the voter's electronic device, unattended ballot dropboxes, US Postal Service, fax services, etc.)

Five Security table comparators are discussed below.

Destruction Evident

[i] *App Based, Digitally Protected & Ledgered Return:* In ledger-based systems, once a ballot is verified & ledgered, its destruction is evident to any party with the ability to view a ledger. However, destruction of a ballot, before the ballot is ledgered, would not be evident.

Preserves Voter Privacy via Permanent Separability

[ii] *Official Paper Ballot Return:* Group members lacked consensus. Some based a "Yes" on the view that physical return methods meet the legal requirement for separation sufficiently for practical purposes, while acknowledging the possibility of insider abuse that would require a careful conspiracy to avoid detection. Some based a "No" on the view that the separability could be undermined by e.g. insider abuse, performing fingerprint analysis and relinking a ballot and affidavit based on matching fingerprints.

[iii] *Voter Printed Ballot Return:* See Endnote 2.

[iv] *App Based, Digitally Protected & Ledgered Return:* Group members lacked consensus. Some based a "Yes" on the view that encrypted ballot and affidavit were not strictly speaking separated, but the encryption could make it difficult to see both ballot and affidavit contents at the same time. Some based a "No" on the view that separation needed to be literal separation, and that cryptographically linked was not tantamount to separation. Some based a "No" on the view that the protection of encryption could be undermined, e.g.,

- by accidental poor key management practice;
- insider abuse to perform unauthorized decryption; or
- future technological breakthroughs (such as quantum computing) to break current encryption schemes in widespread use.

Appendix B: Endnotes for Security Points of Comparison

Post-Election Audit of Voters' Original Ballots

[v] *Voter Printed Ballot Return:* Ballots that require the LEO to transcribe the voter's intent onto a ballot readable by election systems' optical scanners do not allow the voter to physically verify the accuracy of the tabulated ballot. A printed ballot is auditable only when the voter's original ballot is matched to the transcribed and tabulated ballot.

Human Ballot Physical Proximity Required for Tampering

[vi] *App Based, Digitally Protected & Ledgered Return:* In cases where the return method requires hardware support, risks to tampering are limited to devices that contain a secure hardware chip and restricted operating environment to make remote attacks on an encrypted marked ballot impossible.

Group-limited Threat Actor Scale

[vii] *Official Paper Ballot Return:* Group members lacked consensus. Some based a "Yes" on the view that wholesale attacks to modify all paper absentee ballots were infeasible in practice. Most members of the group contend that such attacks are feasible and have occurred. They argue that a "No" indicates the feasibility of a wholesale attack. For example, a syndicate with a compromised insider that swaps out ballots with counterfeit marked ballots.

[viii] *Voter Printed Ballot Return:* Same as Endnote vii

[ix] *App Based, Digitally Protected & Ledgered Return:* Group members lacked consensus. Some based a "Yes" on the view that a wholesale attack on digitally ledgered ballots is infeasible due to the distributed nature of a digital ledger, which is typically spread out over a large geographic area.