

Virginia State Board of Elections  
**Advanced UOCAVA Solutions Research  
Project**

---

*Discussion of the Secure Electronic Return of  
Election Material for Voters Specified in §24.2-  
700 (2) and Military Voters with Disabilities or  
Injuries*

---

**Discussion provided by**  
Scytl USA  
Election Systems and Software

# 1 Executive Summary

As of 2008, estimates indicate that there are between six and seven million Americans who are overseas, in the Armed Forces, or dependents of Armed Forces members residing away from their voting jurisdiction of record. Specifically, the GAO reports that the Uniformed and Overseas Absentee Voting Act (UOCAVA) covers more than 6.5 million people, including approximately 3.7 million overseas citizens not affiliated with the government (about 2 million of which are of voting age), 1.4 million military service members, and 1.3 million military dependents of voting age. As of January 2012, Virginia has 3,000 UOCAVA voters and protects these voters under the Code of Virginia § 24.2-700 (2). These American citizens include soldiers stationed in places such as Iraq and Afghanistan, who are currently fighting the war against terrorism; missionaries working in remote regions of the world; younger Americans studying abroad; and Americans who work overseas, building economic opportunities in the global economy.<sup>1</sup> In addition to voting from remote locations, many military service members are further challenged with physical and mental impairments as a result of their service.

As chronicled in *No Time to Vote*<sup>2</sup> – a study by the Pew Charitable Trusts - these voters have traditionally had difficulty with full participation in the electoral process. Most notably, military and overseas voters tend to experience difficulties with receiving and returning their ballots in a timely and reliable manner. Technology of varying sorts presents possible improvements to the process and assistance to UOCAVA voters who experience these difficulties. Two of the most important questions being raised about these technologies are 1) whether they are a secure alternative to the traditional absentee ballot system and 2) whether they can also assist those voters who have suffered physical and mental wounds from their service. This discussion paper will introduce some of the technologies available for improving UOCAVA voting and work through an assessment of how each ballot return technology addresses security risks and provides accessibility assistance to these voters. The discussion will remain at a high-level and is meant to provide insight into which of these technologies offer the most potential.

The organization of this document is the following:

- Section 1 explains the objectives of this discussion and the outcome of the assessment.
- Section 2 describes the voting return channels to be assessed and the methodology used to assess them.
- Sections 3 to 6 provide evaluations of the different voting return channels.
- Section 7 contains the conclusions of this discussion paper.
- Section 8 includes additional resources or referents.

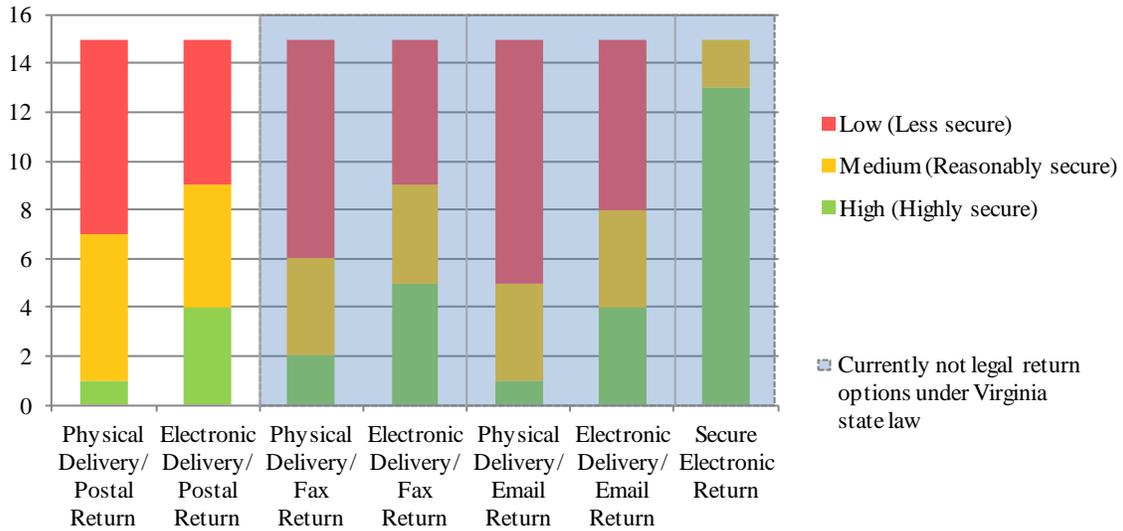
The discussion and assessment in this paper concludes that the secure electronic return option holds the most potential for addressing the traditional UOCAVA voting difficulties while providing an accessible platform for those voters with disabilities. It provides the same – often times better – security protections as that of postal voting while greatly increasing the ability for voters with disabilities to vote in an independent and private manner. The following charts provide a synopsis of the discussion.

---

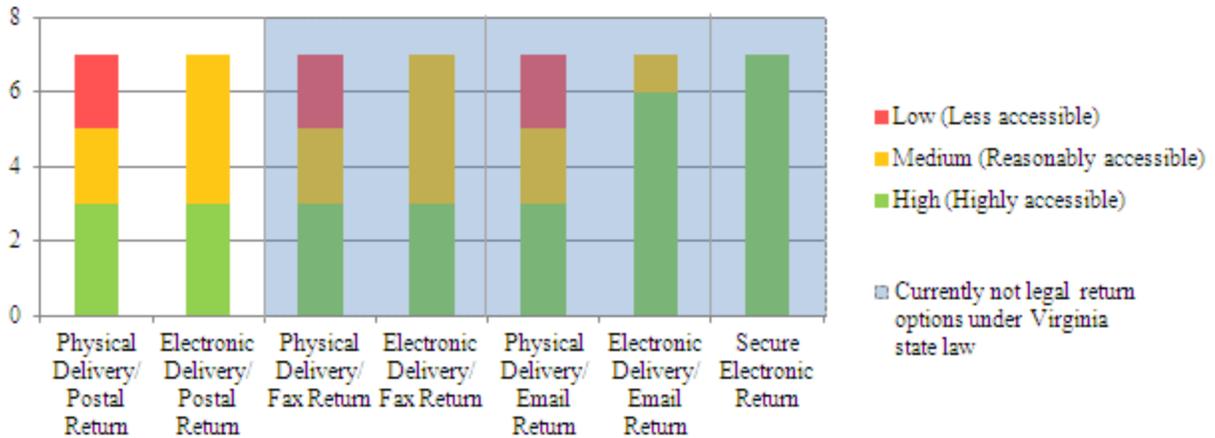
<sup>1</sup> [Thad Hall. UOCAVA: A State of Research.](#)

<sup>2</sup> [Pew Charitable Trusts. No Time to Vote.](#)

**Security assessment per ballot return technology (summary)**



**Accessibility assessment per ballot return technology (summary)**



*Note:* Above charts summarize the ratings assigned in the following sections. The assessment methodology and categories are described in section 2. Tables summarizing these values can be found in Appendix A: Summary assessment tables.

**What is the Advanced UOCAVA Solutions Research Project?**

*The Advanced UOCAVA Solutions Research Project is designed to further the body of knowledge and strengthen the concepts and technology of advanced UOCAVA solutions. These solutions offer great potential for improving the opportunities and reliability for overseas military and civilians to vote in our elections. This project will be targeted at specific technology enhancements in the context of Virginia requirements but will consider application to other similar jurisdictions. Advanced solutions will be examined and piloted in the following technology categories for their significance, sustainability, impact, and scalability – remote voting accessibility, secure electronic return, and mobile voting stations.*

## 2 Comparing UOCAVA Absentee Voting Technologies

The following is a comparison of various absentee ballot return technologies (or return channels) which are currently available to UOCAVA voters to return their ballots:

1. **Postal return.** Postal voting is the use of the postal ballot as a comprehensive alternative to attendance voting. Instead of having a day on which voters attend polling booths to cast their votes, they receive a ballot paper by postal mail and then have a period in which to return their vote by mail before Election Day.
2. **Fax return.** Fax voting consists of transmitting the ballot by fax to a pre-assigned number. This channel is mainly supported as a contingency measure in case voters cannot cast their votes on time.
3. **Email return.** This channel requires voters to send an email with a scanned version of their ballot (PDF formatted) attached. This email is sent to the local election official's email address. If the ballot is accepted, the emailed vote (PDF) is printed by the election official and put into an envelope to keep it safe until it is counted.
4. **Secure electronic return.** This channel is defined as an election system using electronic ballots to allow voters to transmit their voted ballot to election officials over the Internet.

The comparison looks at how each return technology addresses the need to provide a secure and accessible return channel. The level of security will be measured by how well the technology addresses the security risks associated with absentee voting. The level of accessibility then will be measured by the availability of personal assistive devices for common voter disabilities.

Each return technology will be given a rating based on how well it has addressed each security risk and the availability of personal assistive devices for each disability type. The rating categories will be the following:

- **High (or highly secure).** The requirement is totally fulfilled and the residual risk level is low, considered an acceptable risk for any existing risk level tolerance.
- **Medium (or reasonably secure).** The requirement is partially fulfilled and the residual risk level is medium, considered as moderate.
- **Low (or less secure).** The requirement is not fulfilled and the residual risk level is high, as there are no effective countermeasures to reduce it.

### 2.1 Assessing Security

The following security requirements and related risks will be assessed for each ballot delivery technology option:

- ✓ **Speed of delivery/ballot replacement.** This requirement captures the ability of the delivery channel to deliver the ballot in a timely manner to the voter, taking into consideration the procedures for approval and preparation of the response package, and to deliver a new ballot if the previous delivered one was incorrect, destroyed during transport or otherwise subject to replacement.
- ✓ **Provide correct ballots.** The delivery channel should provide the correct documents to each voter (ballots and additional information related to each eligible voter and its jurisdiction/precinct).
- ✓ **Prevent ballot tampering.** The delivery channel should put mechanisms in place to avoid manipulation of the documents sent to the voter.
- ✓ **Prevent ballot spoofing.** The documents sent by the delivery channel should incorporate a mechanism to validate the authenticity of the documents sent, avoiding the chance of a third party sending illegitimate ballots to the voter.
- ✓ **Ensure proper delivery.** The delivery channel should guarantee an accurate delivery of the ballots, taking into consideration the actual location of the voter.

The follow security requirements and related risks will be assessed for each ballot return technology.

- ✓ **Eligibility.** Only authorized voters should be able to vote. This means that the channel must provide a robust way to identify voters and only allow those so identified to vote. One of the main issues of absentee voting is that voters cannot be identified in person, leaving the opportunity for individuals to impersonate

eligible voters. This discussion distinguishes impersonation in two different categories: voluntary and involuntary. Involuntary impersonation is related to the impersonation of the voter without his/her knowledge (e.g., the theft of the voter credentials required to cast a vote). Voluntary impersonation requires the participation of the voter, who cooperates with the person that will impersonate such voter by providing his/her voting credentials. With the aim to simplify the comparison, we considered the risks of voluntary impersonation in the coercion and vote buying resistance security requirement. Therefore we only evaluated the risks of involuntary impersonation in this eligibility requirement.

- ✓ **Privacy.** The voting system has to protect voter privacy, concealing the relationship between voter and his/her cast vote, and ensuring that the voter's choice will remain anonymous. This requirement must be fulfilled once the voter has cast his/her vote and must be preserved during the counting process.
- ✓ **Integrity.** A voting system has to protect the vote against manipulation once it is cast and until it is counted. Therefore the channel must provide measures to prevent and/or detect any attempt to change the voter's intent once the vote has been cast.
- ✓ **Voter verifiability – cast as intended.** In this discussion, voter verifiability has been divided as: “cast as intended verification” and “counted as cast verification”. In cast as intended, voter must have the possibility to check that his/her vote has been accurately recorded. In the case of absentee voting, this implies the availability to confirm that the ballot received by the election officials and stored in the remote Ballot Box (in a physical or electronic manner) is the same as cast by the voter. It is important to note that this requirement cannot conflict with the others ones (i.e., coercion and vote buying).
- ✓ **Voter verifiability - counted as cast.** In the counted as cast verification, voters must have the possibility to verify the inclusion of his/her vote in the final tally. This is not a requirement currently included in traditional voting methods.
- ✓ **Prevention of intermediate results.** It is important to prevent the disclosure of intermediate results before the election is closed. This measure ensures that all the voters have the same information during the voting stage.
- ✓ **Ballot box accuracy.** Protection of the ballot box against the addition of illegitimate ballots or the elimination of legitimate ballots is required.
- ✓ **Coercion and vote buying resistance.** As introduced before, one of the main concerns of remote voting channels are that they facilitate voter coercion or vote buying. Therefore it is important to assess if the channel facilitates these practices or includes countermeasures to prevent them. The voting channel must mitigate the risks of voluntary impersonation, in which eligible voters cooperate with the coercer or buyer to access the voting system, and involuntary coercion – where the voter is forced to disclose their voting credentials.
- ✓ **Channel reliability.** This requirement captures the ability for the return channel to provide a consistent, dependable, and time sensitive return channel. This requirement also includes the ability for voters to determine if their vote has been received by the electoral authority on time to be tallied. Other factors, such as the risk of denial of service attacks, influence the availability of the channel. Therefore in this criterion we will balance the ability to detect such delays in an appropriate timeframe (e.g., the detection of a denial of service) and the ability to react to them (e.g., use a contingency channel to cast the vote).
- ✓ **Auditing of the election results.** Voting channels must provide means for facilitating the audit of the election to ensure its correct execution. This means that it must allow the verification of the accuracy of the election results and provide the means to resolve any dispute.

## 2.2 Assessing Accessibility

From an accessibility point of view, the main requirement is to ensure that impaired voters are provided independent means to vote with total privacy, without the need of assistance from third parties. Additionally, the following requirements are also analyzed: Prevention of voting errors (the voting channel has to prevent involuntary voting errors by voters when casting their votes – e.g., under-voting, over-voting) and Ease of Use (the voting channel must be easy to use by average voters and by impaired voters as well). The accessibility assessment will be considered per the disability categories below:

- ✓ **Blindness.** Major symptom is the loss of all visual acuity.
- ✓ **Partial visual loss/visual dysfunction.** Major symptoms are altered light perception, loss of sight in one hemisphere, loss of some visual acuity, double vision, blurring, problems focusing, and sensitivity to light.
- ✓ **Deafness.** Major symptoms are complete hearing loss.
- ✓ **Partial hearing loss/tinnitus.** Major symptoms are some hearing loss, dizziness, noise sensitivity, concentration problems, ringing or other noise in ears, irritability, fatigue, concentration problems.
- ✓ **Dexterity (amputation/loss of limb of upper extremities).** Major symptoms are loss of one or more fingers, hands, or arms. This category also includes paralysis/spinal cord injuries such as quadriplegic which result in a partial or total motor and sensory loss of all limbs and torso, other orthopedic injury limiting voluntary movement and severe burns (thermal injury to skin).
- ✓ **Mobility (amputation/loss of limb of lower extremities).** Major symptoms are loss of one or more toes, feet, legs. This category also includes paralysis/spinal cord injuries such as paraplegic which result in an impairment in motor or sensory function of the lower extremities or quadriplegic.
- ✓ **Cognition (behavioral health/TBI).** Major symptoms are:
  - *Behavioral health – PTSD:* flashbacks, intrusive thoughts, nightmares, hyper-arousal, irritability, memory & concentration problems, emotional withdrawal.
  - *Behavioral health – depression:* depressed mood, loss of interest in daily activities, fatigue, feelings of worthlessness, impaired ability to concentrate & make decisions, suicidal ideation.
  - *TBI – mild:* headache, fatigue, memory & concentration problems, irritability.
  - *TBI – moderate/severe:* significant memory & concentration problems, irritability, motor weakness, balance problems, speech deficits, seizures, chronic pain.

Moreover, this discussion on accessibility makes the following assumptions:

- The standard is a private voting session; no assistance from another person should be required.
- Personal assistive devices are assistive technologies which are not cost prohibitive and it is reasonable to assume the voter has access to or could gain access to device easily and knows how to operate them.

### 3 Postal Return of Ballots

The standard vote-by-mail (VBM) model is the most common absentee balloting method in use today to meet UOCAVA requirements. It involves three key steps: 1) ballot request by the voter, 2) delivery of the absentee ballot, and 3) return of the ballot via postal service. Within the vote-by-mail model, there are two delivery methods of the ballot to the voter – physical or electronic delivery.

Physical delivery most commonly involves use of a postal service to transmit the ballot from the jurisdiction to the voter. (For brevity, this discussion is also going to consider facsimile delivery to be equivalent to physical delivery as the security and accessibility considerations are very similar).

Electronic delivery to the voter may be accommodated by an internet portal service where the voter authenticates their identity in order to receive an electronic copy of their ballot, or through direct email transmission of a ballot document from the jurisdiction to the voter. The former is quickly becoming the most widely used electronic delivery mechanism due to the success of the Federal Voting Assistance Program (FVAP) Electronic Voting Support Wizard and Electronic Absentee Systems for Elections projects in 2010 and 2011 respectively. Additionally, the latter (email delivery of the ballot) offers inferior levels of security and traceability. For this discussion, therefore, electronic delivery is assumed to be a secure internet portal service which makes full use of the technological security controls available (i.e. encryption, digital signatures, strong authentication, etc).

The distinguishing feature of the traditional vote-by-mail (postal return) method remains that the physical ballot must be returned via a postal service to the originating jurisdiction. This is most often accomplished through what is termed the two-envelope system where the voter inserts the ballot inside an interior envelope, signs the voter statement, and inserts the interior envelope with the voter statement into an outside mailing envelope. Upon receipt at the local jurisdiction, the identity of the voter is then authenticated through signature verification before the ballot is separated from the voter’s identify and set aside for tabulation. This process protects the privacy of the ballot without compromising the need to determine voter eligibility. Some jurisdictions utilize technologies for voter signature verification that can serve to mitigate the heavy workload of this process. This is most commonly encountered in jurisdictions with large vote-by-mail returns (e.g. the State of Washington). However, this task is traditionally performed through a manual signature comparison of the absentee ballot materials to the voter registration system. Postal return of the absentee ballot may also be required by the jurisdiction as a “backup” or means of verification for absentee voters who utilize one of the other ballot return methods.

#### 3.1 UOCAVA Vote-by-mail (VBM) Security

For each key step in the VBM model, there are inherent risks, subject to current and future attempts to mitigate them. Since the first key step (ballot request by voter) is common and is not dependent on the ballot return method, we will focus on the risks of the second (ballot delivery) and third (ballot return) phases of the VBM model by comparing the postal delivery, electronic delivery, and postal return of ballots.

Table 3-1. Postal Return Channel - Security requirements assessment

Security Factor		Physical Delivery/Postal Return	Electronic Delivery/Postal Return
<b>BALLOT DELIVERY</b>	<b>Speed of Delivery/Ballot Replacement</b>	<p style="text-align: center;"><u>Low (Less secure)</u></p> <p>Lengthy processing time – delivering the physical documents to the voter may take a lengthy period depending on distance and which postal service is utilized, in addition to the lengthy manual process involved in approving and packaging the absentee ballot request.</p> <p>Replacement is difficult – if the ballot is incorrect, destroyed in transport, or otherwise subject to replacement, the manual processes involved must be repeated.</p>	<p style="text-align: center;"><u>High (Highly Secure)</u></p> <p>With electronic delivery, ballots are posted by the local election jurisdiction and pulled from the secure website. As soon as the ballots are posted by the jurisdiction, the voter can login and download the ballot. For replacements, the voter may return and repeat the process.</p>

Security Factor		Physical Delivery/Postal Return	Electronic Delivery/Postal Return
	<b>Provide Correct Ballots</b>	<p><u>Medium (Reasonably secure)</u></p> <p>Incorrect documents provided – since the selection of the correct physical ballot is a manual process, it carries increased risk that the jurisdiction may provide an incorrect ballot to the voter or omit key components of the absentee package.</p>	<p><u>Medium (Reasonably secure)</u></p> <p>Reliant on incorrect data – electronic delivery is reliant on voter and ballot information accuracy as stored in the local voter registration and election management systems. If this data is not correct when provided to the ballot delivery system, voters may not receive the correct ballots.</p>
	<b>Prevent Ballot Tampering</b>	<p><u>Medium (Reasonably secure)</u></p> <p>Physical security of key documents – the security of the VBM process is dependent on the secure transport of the physical documents via postal service, public or private, to the voter.</p>	<p><u>High (Highly Secure)</u></p> <p>With electronic delivery, ballots are available from a secure website, which establishes a secure channel between the voter and the server that does not allow tampering of the ballot sent.</p>
	<b>Prevent Ballot Spoofing</b>	<p><u>High (Highly Secure)</u></p> <p>Ballots are sent inside official mailing envelopes and may contain an official seal on the ballot to represent its authenticity.</p>	<p><u>High (Highly Secure)</u></p> <p>With websites, the ballot spoofing concerns are based on illegitimate websites presenting themselves as official. However, secure websites have multiple ways to present proof of authenticity to voters. First, the use of a digitally signed certificate will authenticate the web server to the voter’s web browser. Second, the web portal can implement a security image which should be verified by the voter when logging in.</p>
	<b>Ensure proper delivery</b>	<p><u>Low (Less secure)</u></p> <p>Address changes – postal delivery relies on the election official having the most recent physical address of the voter in order to send the ballot to the correct location. When this is not the case, the voter may never receive the ballot and/or the ballot may go to an unqualified voter.</p>	<p><u>High (Highly Secure)</u></p> <p>Electronic delivery is not restricted based on the voter’s physical location. Instead, voters can access their ballots from nearly anywhere. Authentication is typically based on something the voters knows or has with them so this also does not pose a restriction on the delivery to the voter.</p>
<b>BALLOT RETURN</b>	<b>Eligibility</b>	<p><u>Low (Less secure)</u></p> <p>Easy involuntary impersonation to cast a vote. Handwritten signatures are difficult to validate accurately or not always validated.</p> <p>With physical delivery, it is also very difficult to assure that the correct voter received the ballot. This is mitigated when using electronic delivery because the voter is authenticated in order to download the ballot.</p>	
	<b>Privacy</b>	<p><u>Medium (Reasonably secure)</u></p> <p>Voter Privacy – the voter’s right to a private ballot is limited to the physical security of the postal service used to transport the ballot to the original jurisdiction and to the procedures followed by the local jurisdiction to open and tabulate the voter’s ballot in a manner which preserves the voter’s privacy.</p>	
	<b>Integrity</b>	<p><u>Low (Less secure)</u></p> <p>Physical security of key documents – the integrity of the voted ballot is subject to the physical security of the means used to transport the ballot to the original jurisdiction. There is no way</p>	

Security Factor	Physical Delivery/Postal Return	Electronic Delivery/Postal Return
	to prove that the cast vote stays unaltered during the election process.	
<b>Voter verifiability - cast as intended</b>	<p style="text-align: center;"><u>Low (Less secure)</u></p> <p>Although there are tools to track a vote sent by mail (counted as cast), there is no guarantee that the envelope received by the election officials contains the same vote cast by the voter, as the voter cannot verify if the ballot contents are the same selected by him/her.</p>	
<b>Voter verifiability - counted as cast</b>	<p style="text-align: center;"><u>Medium (Reasonably secure)</u></p> <p>The voter can verify that his/her ballot is present during the tallying process through a ballot tracker, which is a system updated by the local election jurisdiction when receiving the ballot.</p>	
<b>Prevent intermediate results</b>	<p style="text-align: center;"><u>Medium (Reasonably secure)</u></p> <p>Intermediate results – the physical ballot may be intercepted by a third party in order to ascertain early results.</p>	
<b>Ballot box accuracy</b>	<p style="text-align: center;"><u>Medium (Reasonably secure)</u></p> <p>It is possible to add bogus ballots without detection. Votes can also be eliminated during transportation. However, handwritten signatures can be verified to detect massive fraud.</p>	
<b>Coercion and vote buying resistance</b>	<p style="text-align: center;"><u>Low (Less secure)</u></p> <p>Voter coercion – third parties with access to the voter and the physical ballot may influence the marking of the ballot.</p>	
<b>Channel reliability</b>	<p style="text-align: center;"><u>Low (Less secure)</u></p> <p>Lengthy return time – returning the physical documents to the jurisdiction may take a lengthy period of time, subject to the same constraints as the delivery of materials to the voter.</p> <p>Incorrect documents returned – successful return of the ballot is dependent on the voters’ inclusion of all required materials to the jurisdiction; omission of items may delay the processing of or invalidate the absentee ballot altogether.</p> <p>This voting channel depends on the reliability of the postal system in the country from which votes are cast. It is not unusual to receive votes after the closing date and voters cannot do anything.</p>	
<b>Auditability</b>	<p style="text-align: center;"><u>Low (Less secure)</u></p> <p>Limited auditability – the physical ballot does not provide means for the jurisdiction to detect the alteration or deletion of voter marks that may have occurred in transit.</p>	

### 3.2 UOCAVA Vote-by-mail Accessibility

Voters who utilize the vote by mail absentee balloting method where ballots are delivered by postal mail are not afforded any personal assistive devices other than those available for reading and marking standard paper. The only widely availability technology for reading printed documents is based on Optical Character Recognition (OCR) which requires specific hardware to scan and process the printed document. While the OCR technology is becoming more reliable, it often has difficulty with special characters and complex layouts which are common with ballots.

For voters who receive their ballots electronically through an electronic ballot delivery (EBD) system, there are many more personal assistive devices available to read and mark their ballot through the use of their personal computer. These voters are still forced to print out and submit the ballots via postal mail. This introduces a gap between the time the ballot is printed and placed into the postal system where there are little to no personal assistive

devices which will assist a voter with a disability in properly returning the ballot. A table providing the personal assistive devices available for the postal return channel is presented below.

**Table 3-2. Postal Return Channel – Accessibility assessment**

Impairment Type	Physical Delivery/Postal Return	Electronic Delivery/Postal Return
<b>Blindness</b>	<p style="text-align: center;"><u>Low (Less secure)</u></p> <p>Few assistive devices are available for reading a paper ballot much less marking and returning it. For reading the ballot, there are technologies available to convert the type font on the paper to auditory sounds. This technology requires a scanner and optical character recognition software in order to transcribe the text into audible words. However, in the case of ballots with several races and complex layout, it may be complicated to reproduce the ballot without introducing errors into audible words.</p> <p>In a remote voting environment, there is no assistive device for marking a paper ballot, reviewing the marks, and returning it.</p>	<p style="text-align: center;"><u>Medium (Reasonably secure)</u></p> <p>The following are assistive devices which are widely available for remote voters with blindness to read, mark, and review their ballots on a computer.</p> <ul style="list-style-type: none"> <li>• Screen reader (interprets the page’s HTML code and reproduces its content as speech correctly for the voter).</li> <li>• Headphones with adjustable volume.</li> <li>• Standard keyboard – the website supports keyboard-based navigation and selection (i.e. no mouse required).</li> <li>• Reduced keyboard (numeric keyboard) with access to all voting functionalities.</li> <li>• Keyboard with Braille embossed – keyboards can be equipped with braille stickers to indicate each key for navigation and selection on the website.</li> </ul> <p>The voter must still print his or her ballot, sign the voter statement, and return the ballot via postal mail.</p>
<b>Partial visual loss / visual dysfunction</b>	<p style="text-align: center;"><u>Medium (Reasonably secure)</u></p> <p>There are traditional and computer enhanced magnifiers to assist with reading, marking, reviewing, and returning the ballot. There is no ability, however, to adjust the contrast ratio of the printed ballot.</p>	<p style="text-align: center;"><u>Medium (Reasonably secure)</u></p> <p>The same personal assistive devices are available for electronic delivery as those referenced above for blindness plus the ability to adjust the contrast ratio of the images and text on the website and use an independent screen magnifier (adjustable entire screen contrasts, color and font sizes).</p> <p>The voter must still print and sign the voter statement before inserting the ballot into the return envelope for postal return.</p>
<b>Deafness</b>	<p style="text-align: center;"><u>High (Highly Secure)</u></p> <p>There is no auditory requirement for reading, marking, reviewing, or returning a paper ballot.</p>	<p style="text-align: center;"><u>High (Highly Secure)</u></p> <p>There is no auditory requirement for reading, marking, reviewing, or returning an electronically delivered paper ballot.</p>
<b>Partial hearing loss / tinnitus</b>	<p style="text-align: center;"><u>High (Highly Secure)</u></p> <p>There is no auditory requirement for reading, marking, reviewing, or returning a paper ballot.</p>	<p style="text-align: center;"><u>High (Highly Secure)</u></p> <p>There is no auditory requirement for reading, marking, reviewing, or returning a paper ballot.</p>
<b>Dexterity (amputation/loss of limb of upper extremities)</b>	<p style="text-align: center;"><u>Low (Less secure)</u></p> <p>There are no widely available personal assistive devices to assist voters with dexterity impairments in physically marking the paper ballots. It is also difficult for these voters to sign the voter statement and enclose their ballot properly for return.</p>	<p style="text-align: center;"><u>Medium (Reasonably secure)</u></p> <p>The following are assistive devices which are widely available for remote voters with dexterity impairments to use to read, mark, and review their ballots on a computer.</p> <ul style="list-style-type: none"> <li>• Sip and puff device (simple and effective way to control mouse button clicking/mouse movement).</li> <li>• Head mouse (mouse controlled with the head).</li> <li>• Screen/virtual keyboard.</li> </ul>

Impairment Type	Physical Delivery/Postal Return	Electronic Delivery/Postal Return
		<ul style="list-style-type: none"> <li>• External devices emulating mouse and keyboard.</li> </ul> <p>The voter must still print his or her ballot, sign the voter statement, and return the ballot via postal mail.</p>
<p><b>Mobility (amputation/loss of limb of lower extremities)</b></p>	<p><u>High (Highly Secure)</u></p> <p>There are no mobility requirements for reading, marking, reviewing, and returning an absentee paper ballot which was delivered to the voter's location.</p>	<p><u>High (Highly Secure)</u></p> <p>There are no mobility requirements for reading, marking, reviewing, and returning an absentee paper ballot which was downloaded to the voter's personal computer.</p>
<p><b>Cognition (behavioral health / TBI)</b></p>	<p><u>Medium (Reasonably secure)</u></p> <p>Paper ballots are well understood because of their pervasiveness but they do not provide much assistance to voters with cognitive impairments. The use of clear, brief instructions and a simple ballot layout is the best approach.</p>	<p><u>Medium (Reasonably secure)</u></p> <p>Electronic delivery of ballots has a number of mechanisms it can use to assist those voters with cognitive impairments. Beyond what can be done on the electronic ballot delivery service, the voter will still have to print and assemble the return envelopes according to the standard instructions in order to properly return the ballot. A few examples are included below:</p> <ul style="list-style-type: none"> <li>• Use of common images to help recognize instructions and ballot content.</li> <li>• Use of common colors and font types to represent important concepts.</li> <li>• Use of common sounds and signals to signify the completion of an event.</li> <li>• Use of simple written instructions.</li> <li>• Use of simple verbal instructions.</li> <li>• Use of step by step processes (i.e. break down complex ballot marking into smaller steps).</li> <li>• Provide longer explanations for tasks, as necessary.</li> <li>• Provide warnings for common voter mistakes, such as under-voting and over-voting.</li> </ul>

## 4 Fax Return of Ballots

*Note: Although this is not currently a legal return option under Virginia state law, various other states do support this return method for UOCAVA voters. Therefore, the discussion paper assumes its legality solely for purpose of comparison*

Another method of returning an absentee ballot utilizes facsimile transmission of the physical ballot from the voter to the originating jurisdiction. This method improves upon the time constraints of the traditional VBM process since receipt of the voted ballot is no longer limited by the speed of the postal service(s) involved. Rather, the image of the voted ballot is captured and sent to the jurisdiction using machines that transmit over traditional analog phone-lines or digital facsimile service.

### 4.1 UOCAVA Fax Return Security

Typically, if this method is allowed by a jurisdiction, it requires that the voter submit additional documentation, primarily an agreement that their right to a secret ballot has been waived. Since the ballot is transmitted in the clear, unlike the traditional postal channel where the secrecy of the voted ballot is preserved, alongside the voter's identification, there is no longer a reasonable expectation that their votes can be kept independent of their identity at the time when the ballot is received. After confirmation of the voter's registration, however, the ballot is sealed and set aside for tabulation. The voter may also be required by the jurisdiction to transmit the original physical ballot to the jurisdiction by postal service as an additional step. The following table details the security afforded to facsimile return. Refer to Table 3-1 for the security assessment for the physical and electronic delivery.

**Table 4-1. Fax Return Channel – Security requirements assessment**

Security Factor	Fax Return (physical delivery or electronic delivery)
<p><b>Eligibility</b></p>	<p style="text-align: center;"><u>Low (Less secure)</u></p> <p>Easy involuntary impersonation to cast a vote. Handwritten signatures are digitized and therefore easy to tamper with.</p> <p>With physical delivery, it is also very difficult to assure that the correct voter received the ballot. This is mitigated when using electronic delivery because the voter is authenticated prior to downloading the ballot.</p>
<p><b>Privacy</b></p>	<p style="text-align: center;"><u>Low (Less secure)</u></p> <p>Votes are received without any privacy protection. Voters are required to sign a secrecy waiver.</p> <p>The voter's right to a private ballot is lost since the facsimile transmission method cannot separate the ballot from the registration information.</p>
<p><b>Integrity</b></p>	<p style="text-align: center;"><u>Low (Less secure)</u></p> <p>There is no way to prove that the cast vote stays unaltered during the election process.</p>
<p><b>Voter verifiability - cast as intended</b></p>	<p style="text-align: center;"><u>Low (Less secure)</u></p> <p>There is no guarantee that the fax vote is received at the destination as it was cast by the voter and there are no mechanisms for the voter to verify if the received ballot contents are the same selected by him/her.</p>
<p><b>Voter verifiability - counted as cast</b></p>	<p style="text-align: center;"><u>Medium (Reasonably secure)</u></p> <p>The voter can verify that his/her ballot is present during the tallying process through a ballot tracker, which is a system updated by the local election jurisdiction when the ballot is accepted.</p>
<p><b>Prevent intermediate results</b></p>	<p style="text-align: center;"><u>Low (Less secure)</u></p>

Security Factor	Fax Return (physical delivery or electronic delivery)
	Vote contents could be accessed during the transmission. The vote contents are always accessible upon reception.
<b>Ballot box accuracy</b>	<p style="text-align: center;"><u>Medium (Reasonably secure)</u></p> It is possible to add bogus ballots without detection. However, the fax numbers of the voters can be audited in order to detect mass fraud.
<b>Coercion and vote buying resistance</b>	<p style="text-align: center;"><u>Low (Less secure)</u></p> Voters can show the selected voting options to third parties before casting their votes, making coercion and vote selling possible.
<b>Channel reliability</b>	<p style="text-align: center;"><u>High (Highly Secure)</u></p> Voters realize if their fax vote has not reached the election authority. Therefore contingency measures (e.g., try later or use another voting channel) can be used to prevent the loss of their votes.  Incorrect documents returned – mitigated in part through the shorter delivery time; this allows the voter to more easily rectify the missing or incorrect documentation.
<b>Auditability</b>	<p style="text-align: center;"><u>Low (Less secure)</u></p> Voting channel (land phone) is difficult to audit and does not generate enough trails to solve any dispute and to audit the entirety of the election process to ensure its correct execution. Moreover, the facsimile ballot image does not provide means to detect the alteration or deletion of voter marks on the ballot.

## 4.2 UOCAVA Fax Return Accessibility

If a voter chooses to return their voted ballot by fax, he or she is going to be afforded nearly identical accessibility assistance as a voter who is returning their ballot by postal mail. There is one notable exception to this, however, if the voter is receiving the ballot electronically. There are programs available which would allow the voter to fax his ballot without ever having to print the ballot PDF. There are numerous security concerns with this, but no more so than returning the ballot by traditional fax. By keeping the ballot completely digitized, this vastly increases the number of personal assistive devices which the voter can utilize. The voter would still have to return other statements with his or her ballot which would require the voter’s signature. So long as digital signatures are not accepted, the voter would have to print out, sign the voter statement, and scan it into the computer in order to fax it along with the ballot. As one can see, there are some possible improvements to accessibility with the fax return channel but none which represent a definitively better alternative for voters. Therefore, the discussion concludes that the same accessibility scores will be given to the fax return channel as with postal return (reference

Table 3-2 for this analysis).

## 5 Email Return of Ballots

*Note: Although this is not currently a legal return option under Virginia state law, various other states do support this return method for UOCAVA voters. Therefore, the discussion paper assumes its legality solely for purpose of comparison*

Another technologically available method for the return of an absentee ballot is via email service over public email exchanges. As with postal and facsimile returns, the ballot may be initially delivered to the voter through physical or electronic means. The email return process itself may take two slightly different forms: email transmission of a scanned image of the original ballot or email transmission of an electronic ballot document (e.g. a .PDF image of the ballot). If the ballot is provided to the voter via postal service, conversion into an electronic copy presents an additional hurdle to the voter because it will have to be scanned into the computer. However, the presence of a physical copy does allow for the voter to return the original ballot document as a supplement to their electronic return. If the voter marks and downloads the ballot from an electronic delivery service, the voter can attach the ballot directly to an email. It is important to mention that the voter will likely still be required to sign, scan and attach the voter statement to the email as well. This will require the voter to use a printer and scanner. Unfortunately, this impacts the overall appeal of the email option as detailed in the security and accessibility analysis below.

### 5.1 Email Return Security

The security of the ballot delivery options was discussed previously and detailed in Table 3-1. Therefore, this section will focus on the security controls afforded to ballots using email as the return channel.

In this discussion of email return, the use of an encryption client is not being considered because, in order for it to be securely used, the voter and election official have to share a cryptographic key or the election official has to setup a PKI (public key infrastructure). This is a difficult implementation and is prone to error, even with expert assistance. Furthermore, the discussion concludes that if the encryption system is strong enough, it will likely resemble a secure electronic return option and will no longer be considered email return. The assessment for standard email return security is below.

**Table 5-1. Email Return Channel – Security requirements assessment**

Security Factor	Email Return (physical delivery or electronic delivery)
<b>Eligibility</b>	<p style="text-align: center;"><u>Low (Less secure)</u></p> <p>Easy involuntary impersonation to cast a vote. Handwritten signatures are digitized and therefore easy to tamper with.</p> <p>With physical delivery, it is also very difficult to assure that the correct voter received the ballot. This is mitigated when using electronic delivery because the voter is authenticated in order to download the ballot.</p>
<b>Privacy</b>	<p style="text-align: center;"><u>Low (Less secure)</u></p> <p>Votes are received without any privacy protection. Voters are required to sign a secrecy waiver.</p> <p>The voter’s right to a private ballot is lost since the email transmission method cannot separate the ballot from the registration information.</p>
<b>Integrity</b>	<p style="text-align: center;"><u>Low (Less secure)</u></p> <p>There is no way to prove that the cast vote stays unaltered during the election process.</p>
<b>Voter verifiability - cast as intended</b>	<p style="text-align: center;"><u>Low (Less secure)</u></p> <p>The voter does not have any means to individually verify that the email vote is received at the destination as it was cast by the voter and there are no mechanisms for the voter to verify if the received ballot contents are the same as those selected by him/her.</p>
<b>Voter verifiability -</b>	<p style="text-align: center;"><u>Medium (Reasonably secure)</u></p>

<b>Security Factor</b>	<b>Email Return (physical delivery or electronic delivery)</b>
<b>counted as cast</b>	The voter can verify that his/her ballot is present during the tallying process through a ballot tracker, which is a system updated by the local election jurisdiction when the ballot is accepted.
<b>Prevent intermediate results</b>	<u>Low (Less secure)</u> Vote contents could be accessed during the transmission. The vote contents are always accessible upon reception.
<b>Ballot box accuracy</b>	<u>Low (Less secure)</u> It is possible to add bogus ballots. Email addresses can be impersonated. Emails can be eliminated during transmission.
<b>Coercion and vote buying resistance</b>	<u>Low (Less secure)</u> Voters can show the selected voting options to third parties before casting their votes, making coercion and vote selling possible.
<b>Channel reliability</b>	<u>Medium (Reasonably secure)</u> E-mail reception confirmation can be sent to the voter. However the e-mail transmission can be delayed. Incorrect documents returned – mitigated in part through the shorter delivery time; this allows the voter to more easily rectify the missing or incorrect documentation.
<b>Auditability</b>	<u>Low (Less secure)</u> Voting channel (mailers, DNS servers, etc.) is difficult to audit and does not generate enough trails to solve any dispute and to audit the entirety of the election process to ensure its correct execution.

## 5.2 Email Return Accessibility

The email return of ballots requires that the voter return the ballot in a digital form. This increases the chances that a voter with disabilities will have access to one or more personal assistive devices which may assist him or her with reading, reviewing, and returning the ballot. Whether the ballot is physically delivered or electronically delivered, the chances are that the voter will interact with the ballot at some point when it is in Portable Document Format (PDF). This is the most common file exchange format and the most common program for viewing a PDF is Adobe Reader. Fortunately, Adobe Reader offers the ability for screen readers and other personal assistive technologies to work with the PDFs. That said, Adobe and other PDF readers are often limited in the accessibility support depending on how the PDF file was created. This is actually quite important for this discussion because a downloaded PDF document will be substantially more accessible than ones which are created from a scanned paper document. This consideration and others are discussed in further detail in the table below.

**Table 5-2. Email Return channel – Accessibility assessment**

<b>Impairment Type</b>	<b>Physical Delivery/Email Return</b>	<b>Electronic Delivery/Email Return</b>
<b>Blindness</b>	<u>Low (Less secure)</u> There is nothing inherent in the email return option which affords the voter any more assistance than if returning the paper ballot by mail. If the voter wishes to have the ballot contents read aloud, the voter will still need to scan the ballot into a computer with optical character recognition abilities. This will convert the	<u>High (Highly Secure)</u> The following are assistive devices which are widely available for remote voters with blindness to use to read, mark, review, and return their ballots on a computer. With email return, the ballot does not have to be printed and the voter can therefore review the ballot in PDF form prior to returning it via email. <ul style="list-style-type: none"><li>• Screen reader (interprets the page’s HTML code</li></ul>

Impairment Type	Physical Delivery/Email Return	Electronic Delivery/Email Return
	<p>printed text into digital words and sentences. This will have some success at reading the ballot contents but the success rates vary and become lower the more complex the original document is. In any case, the OCR technology will not be able to verbally indicate a marked or unmarked oval/square to the voter so there is no way for the voter to confirm his or her selections prior to sending the email.</p>	<p>and the PDF and reproduces its content as speech correctly for the voter). In this case, the screen reader clearly indicates whether each race is marked or unmarked.</p> <ul style="list-style-type: none"> <li>• Headphones with adjustable volume.</li> <li>• Standard keyboard – the website supports keyboard-based navigation and selection (i.e. no mouse required).</li> <li>• Reduced keyboard (numeric keyboard) with access to all voting functionalities.</li> <li>• Keyboard with Braille embossed – keyboards can be equipped with Braille stickers to indicate each key for navigation and selection on the website.</li> </ul>
<p><b>Partial visual loss / visual dysfunction</b></p>	<p style="text-align: center;"><u>Medium (Reasonably secure)</u></p> <p>Prior to scanning the ballot into the computer, there are traditional and computer enhanced magnifiers to assist with reading, marking, and reviewing the ballot. Once the ballot is scanned in, the voter can use a screen magnifier to review the ballot, attach it to an email, and send the email.</p> <p>There are still very few assistive technologies in regards to marking the ballot. For example, there is no alternative to a pen/pencil to mark the ballot, such as one that uses Braille or large icons.</p>	<p style="text-align: center;"><u>High (Highly Secure)</u></p> <p>The same personal assistive devices are available for electronic delivery as those referenced above for blindness plus the ability to adjust the contrast ratio of the images and text on the website and use an independent screen magnifier (adjustable entire screen contrasts, color and font sizes). Since the ballot will be returned by email, the voter will be able to use these technologies throughout the entire process. The only drawback here is that the voter will have to move the ballot from one application (the electronic ballot delivery website) to the email client. This will most likely use PDF to transfer the ballot which will have separate accessibility provisions than the EBD website.</p>
<p><b>Deafness</b></p>	<p style="text-align: center;"><u>High (Highly Secure)</u></p> <p>There is no auditory requirement for reading, marking, reviewing, or returning a paper ballot by email.</p>	<p style="text-align: center;"><u>High (Highly Secure)</u></p> <p>There is no auditory requirement for reading, marking, reviewing, or returning an emailed ballot.</p>
<p><b>Partial hearing loss / tinnitus</b></p>	<p style="text-align: center;"><u>High (Highly Secure)</u></p> <p>There is no auditory requirement for reading, marking, reviewing, or returning a paper ballot by email.</p>	<p style="text-align: center;"><u>High (Highly Secure)</u></p> <p>There is no auditory requirement for reading, marking, reviewing, or returning an emailed ballot.</p>
<p><b>Dexterity (amputation/loss of limb of upper extremities)</b></p>	<p style="text-align: center;"><u>Low (Less secure)</u></p> <p>There are no widely available personal assistive devices to assist voters with dexterity impairments in physically marking the paper ballots or scanning it into the computer to email.</p>	<p style="text-align: center;"><u>High (Highly Secure)</u></p> <p>The following are assistive devices which are widely available for remote voters with dexterity impairments to use to read, mark, and review their ballots on a computer. The voter should be able to use these devices to download the PDF from the electronic delivery website and attach it to an email. It may require more steps than preferred (switching applications) but it will be possible with these assistive devices:</p> <ul style="list-style-type: none"> <li>• Sip and puff device (simple and effective way to control mouse button clicking/mouse movement).</li> <li>• Head mouse (mouse controlled with the head).</li> <li>• Screen/virtual keyboard.</li> <li>• External devices emulating mouse and keyboard</li> </ul>

Impairment Type	Physical Delivery/Email Return	Electronic Delivery/Email Return
<p align="center"><b>Mobility (amputation/loss of limb of lower extremities)</b></p>	<p align="center"><u>High (Highly Secure)</u></p> <p>There are no mobility restrictions for reading, marking, reviewing, and returning an absentee paper ballot which was delivered to the voter's location and is being returned via email.</p>	<p align="center"><u>High (Highly Secure)</u></p> <p>There are no mobility restrictions for reading, marking, reviewing, and returning an absentee paper ballot which was downloaded to the voter's personal computer and returned via email.</p>
<p align="center"><b>Cognition (behavioral health / TBI)</b></p>	<p align="center"><u>Medium (Reasonably secure)</u></p> <p>Paper ballots are well understood because of their pervasiveness but they do not provide much assistance to voters with cognitive impairments. This is exacerbated by the use of email clients and the scanners required to convert the ballot to a digital image.</p>	<p align="center"><u>Medium (Reasonably secure)</u></p> <p>Electronic delivery of ballots has a number of mechanisms it can use to assist those voters with cognitive impairments. Beyond what can be done on the electronic ballot delivery service, the voter will still have to attach the ballot to an email and follow other instructions in order to properly return the ballot. A few examples are included below:</p> <ul style="list-style-type: none"> <li>• Use of common images to help recognize instructions and ballot content.</li> <li>• Use of common colors and font types to represent important concepts.</li> <li>• Use of common sounds and signals to signify the completion of an event.</li> <li>• Use of simple written instructions.</li> <li>• Use of simple verbal instructions.</li> <li>• Use of step by step processes (i.e. break down complex ballot marking into smaller steps).</li> <li>• Provide longer explanations for tasks, as necessary.</li> <li>• Provide warnings for common voter mistakes, such as under-voting and over-voting.</li> </ul>

## 6 Secure Electronic Return

*Note: Although this is not currently a legal return option under Virginia state law, various other states allow for and are pursuing this return method for UOCAVA voters. Therefore, the discussion paper assumes its legality solely for purpose of comparison*

Secure electronic return is a return channel that uses electronic ballots and allows voters to transmit the voted ballot to election officials over the internet. This option has been used in various locations in the United States and across the world to aid overseas voters in completing the absentee voting process in a quick, accessible, and secure manner. This return channel relies on electronically delivery of ballots through a secure online system. These ballots are marked by the voter then subsequently encrypted and digitally signed for secure transmission. There are many variants of how secure electronic return can be implemented. Each variant represents a unique cost, usability, and security balance. The analysis below will assume the most advanced implementation which is known as a Remote End-To-End Verifiable eVoting System.

### 6.1 Secure Electronic Return Channel Security

Secure Electronic Return technology is often based on the use of advanced cryptography to achieve the unique security requirements of voting from a remote location. Many of the technologies employ the use of proven cryptographic primitives such as hash functions, digital signatures, and public key cryptography. The most recent and revolutionary techniques utilize homomorphic properties present in certain cryptosystems to achieve end-to-end verifiability. This concept provides both voters and universal auditors with the ability to verify the accuracy of an electronic return system without violating any other requirements, such as voter privacy. These advances in secure electronic return technology are considered below in this assessment.

The security of the ballot delivery options was discussed previously and detailed in Table 3-1. Therefore, this section will focus on the security controls afforded to ballots using secure electronic return as the return channel.

**Table 6-1. Secure Electronic Return Channel – Security requirements assessment**

Security Factor	Secure Electronic Return
<b>Eligibility</b>	<u>High (Highly Secure)</u> The use of strong authentication such as digital certificates prevents the involuntary impersonation of voters.
<b>Privacy</b>	<u>High (Highly Secure)</u> Votes are encrypted before being cast. Cryptographic measures, such as random mixing processes, can be implemented to break any connection between vote and voter. Additionally, voters can protect their PC's against malware or use secure voting kiosks, but it is a voter's choice.
<b>Integrity</b>	<u>High (Highly Secure)</u> Votes can be digitally signed, preventing any manipulation. Furthermore, when using voting receipts, any attempt to delete a vote could be detected by the voter when verifying the receipt. Additionally, voters can protect their PC's against malware or use secure voting kiosks
<b>Voter verifiability - cast as intended</b>	<u>High (Highly Secure)</u> A verification process can be implemented as an independent process from the vote selection process in the voting terminal, which allows the voters to check if the vote received by the election officials and stored in the remote Ballot Box is the same as cast by the voter. Votes are protected by cryptographic means after being cast.
<b>Voter verifiability - counted as cast</b>	<u>High (Highly Secure)</u> A voting receipt can be generated from the digital signature of the encrypted ballot, which allows voters to individually verify that their votes are present in the tallying process.

Security Factor	Secure Electronic Return
<b>Prevent intermediate results</b>	<p style="text-align: center;"><u>High (Highly Secure)</u></p> <p>Votes are encrypted before they are cast. Only the authorized officials of the jurisdiction can decrypt them at the end of the election.</p>
<b>Ballot box accuracy</b>	<p style="text-align: center;"><u>High (Highly Secure)</u></p> <p>Each encrypted vote can be digitally signed using a unique voter digital certificate to prevent the addition of bogus votes. Additionally, voting receipts can be provided to voters to allow them to detect the elimination of their votes.</p>
<b>Coercion and vote buying resistance</b>	<p style="text-align: center;"><u>Medium (Reasonably secure)</u></p> <p>By providing a mechanism that allows voters to self-spoil their ballots and cast replacements, the risk of voter coercion is severely diminished. Voter coercion and voting buying schemes are highly dependent on forcing the voter to provide “proof” of the contents of the final ballot or forcing the use of a premarked ballot on the voter. Self-spoiling eliminates this possibility.</p>
<b>Channel reliability</b>	<p style="text-align: center;"><u>High (Highly Secure)</u></p> <p>Voters realize if their vote has not reached the election authority if an error arises when casting the vote. Therefore contingency measures (e.g., try later or use another voting channel) can be used to prevent the lost of their votes.</p>
<b>Auditability</b>	<p style="text-align: center;"><u>High (Highly Secure)</u></p> <p>Voters can individually check the accuracy of the election with their voting receipts. Auditors can audit the voting application using independent calculation of homomorphic proofs.</p>

## 6.2 Secure Electronic Return Channel Accessibility

Because the use of a secure electronic return channel is most securely accomplished using a unified system, the voter can interact with a single entirely electronic interface to receive, read, mark, and return their ballot. This provides great benefits for using personal assistive devices throughout the voting process. First, all of the operations are conducted through a web browser. Therefore, so long as the voting application is compliant with Section 508 of the US Rehabilitation Act, the entire interface can be read by a screen reader. Furthermore, the voter can use the keyboard, voice commands, a head-mouse, and other alternative input devices to make selections and navigate the ballot. When finished, the voter can have the ballot as marked read back to him/her and with the click of a button, submit their ballot or modify it (if changes are required after the ballot review). This presents a tremendous ease-of-use advantage over having to download, print and attach the ballot to an email. Below is the analysis of the accessibility options available with secure electronic return.

**Table 6-2. Secure Electronic Return Channel – Accessibility assessment**

Impairment Type	Secure Electronic Return
<b>Blindness</b>	<p style="text-align: center;"><u>High (Highly Secure)</u></p> <p>The following are assistive devices which are widely available for remote voters with blindness to use to read, mark, review, and return their ballots on a computer. With secure electronic return, the ballot does not have to be printed and the voter can review the ballot by having the screen reader read the review screen. As opposed to reading a PDF, the review screen of an electronic ballot delivery/return system can be specially tailored to the voting context.</p> <ul style="list-style-type: none"> <li>• Screen reader (interprets the page’s HTML code and reproduces its content as speech correctly for the voter)</li> <li>• Headphones with adjustable volume</li> </ul>

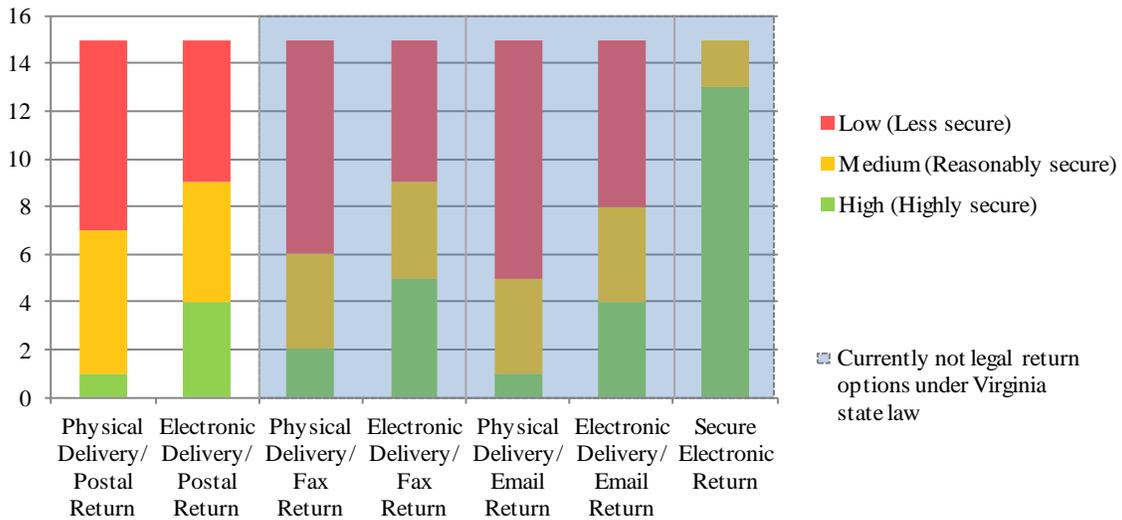
Impairment Type	Secure Electronic Return
	<ul style="list-style-type: none"> <li>• Standard keyboard – the website supports keyboard-based navigation and selection (i.e. no mouse required).</li> <li>• Reduced keyboard (numeric keyboard) with access to all voting functionalities.</li> <li>• Keyboard with Braille embossed – keyboards can be equipped with Braille stickers to indicate each key for navigation and selection on the website.</li> </ul>
<b>Partial visual loss / visual dysfunction</b>	<p style="text-align: center;"><u>High (Highly Secure)</u></p> <p>The same personal assistive devices are available for electronic delivery and secure return as those referenced above for blindness plus the ability to adjust the contrast ratio of the images and text on the website and use an independent screen magnifier (adjustable entire screen contrasts, color and font sizes). Since the entire voting process uses the same system, the voter will be able to use these technologies throughout the entire process.</p>
<b>Deafness</b>	<p style="text-align: center;"><u>High (Highly Secure)</u></p> <p>There is no auditory requirement for reading, marking, reviewing, or returning an electronic ballot.</p>
<b>Partial hearing loss / tinnitus</b>	<p style="text-align: center;"><u>High (Highly Secure)</u></p> <p>There is no auditory requirement for reading, marking, reviewing, or returning an electronic ballot.</p>
<b>Dexterity (amputation/loss of limb of upper extremities)</b>	<p style="text-align: center;"><u>High (Highly Secure)</u></p> <p>The following are assistive devices which are widely available for remote voters with dexterity impairments to use to read, mark, and review their ballots on a computer. The voter will be able to operate these devices to complete the entire voting system on the secure electronic system. This includes receiving, reading, marking, and returning the ballot.</p> <ul style="list-style-type: none"> <li>• Sip and puff device (simple and effective way to control mouse button clicking/mouse movement).</li> <li>• Head mouse (mouse controlled with the head).</li> <li>• Screen/virtual keyboard.</li> <li>• External devices emulating mouse and keyboard.</li> </ul>
<b>Mobility (amputation/loss of limb of lower extremities)</b>	<p style="text-align: center;"><u>High (Highly Secure)</u></p> <p>There are no mobility restrictions for reading, marking, reviewing, and returning an electronic ballot.</p>
<b>Cognition (behavioral health / TBI)</b>	<p style="text-align: center;"><u>High (Highly Secure)</u></p> <p>Electronic delivery of ballots has a number of mechanisms it can use to assist those voters with cognitive impairments. Because the voter will be using the secure electronic system for each step in the voting process, the entire process can use these cognitive assistance techniques to help the voter.</p> <ul style="list-style-type: none"> <li>• Use of common images to help recognize instructions and ballot content.</li> <li>• Use of common colors and font types to represent important concepts.</li> <li>• Use of common sounds and signals to signify the completion of an event.</li> <li>• Use of simple written instructions.</li> <li>• Use of simple verbal instructions.</li> <li>• Use of step by step processes (i.e. break down complex ballot marking into smaller steps).</li> <li>• Provide longer explanations for tasks, as necessary.</li> <li>• Provide warnings for common voter mistakes, such as under-voting and over-voting.</li> </ul>

## 7 Concluding Thoughts

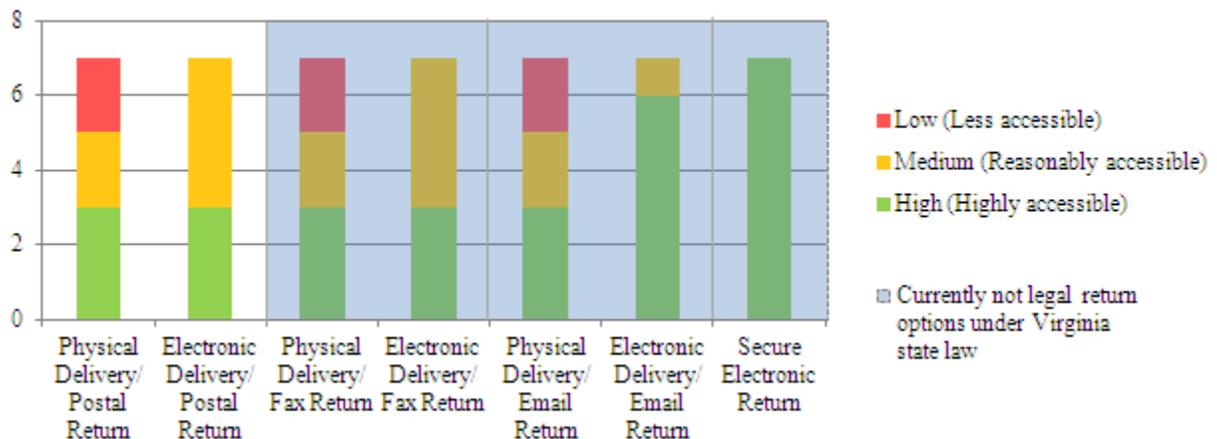
There is a general concern that the use of remote electronic voting channels generates more security issues than postal voting. However, after comparing the different channels used in the United States, we have seen that the secure electronic return voting channel concerns have similar implications as the postal voting ones. Furthermore, secure electronic return allows the implementation of additional security measures (such as cryptographic voting schemes) that can mitigate or, in some cases, eliminate common security risks of the remote voting methods currently accepted in the United States. That does not mean that the secure electronic return channel is free of security risks, but it does provide a better framework for managing those risks (as the residual risk level is low for almost all requirements). Furthermore, it is clear that secure electronic return provides the most access to personal assistive devices to help those voters with disabilities.

Regarding fax and email electronic voting channels, they can pose additional concerns relative to a secure electronic return. The nature of these channels (e.g., the use of unsecured land telephone networks or public email relays) does not effectively serve to enhance the security or accessibility of the voting process beyond that of traditional postal voting. As detailed earlier, in certain cases, these alternate channels may serve only to offset relief in one risk category with increased risk in another.

**Security assessment per ballot return technology (summary)**



**Accessibility assessment per ballot return technology (summary)**



*Note:* Above charts summarize the ratings assigned in the previous sections. Tables summarizing these values can be found in Appendix A: Summary assessment tables.

## 8 Additional Resources

The following additional resources provide more in depth analysis of the return channels security and accessibility provisions.

[http://csrc.nist.gov/groups/ST/UOCAVA/2010/Presentations/PUIGGALI\\_SecurityPractices\\_UOCAVA.pdf](http://csrc.nist.gov/groups/ST/UOCAVA/2010/Presentations/PUIGGALI_SecurityPractices_UOCAVA.pdf)

[http://csrc.nist.gov/groups/ST/UOCAVA/2010/PositionPapers/PUIGGALI\\_BestPracticesInternetVoting.pdf](http://csrc.nist.gov/groups/ST/UOCAVA/2010/PositionPapers/PUIGGALI_BestPracticesInternetVoting.pdf)

[http://csrc.nist.gov/groups/ST/UOCAVA/2010/Presentations/KING\\_UOCAVA\\_Vote\\_by\\_Mail.pdf](http://csrc.nist.gov/groups/ST/UOCAVA/2010/Presentations/KING_UOCAVA_Vote_by_Mail.pdf)

<http://www.scytl.com/images/upload/home/PNYXCOREWhitePaper.pdf>

## Appendix A: Summary assessment tables

### Appendix A.1: Security assessment table

Requirement		Postal Return		Fax Return		Email return		Secure Electronic Return
		Physical Delivery	Electronic Delivery	Physical Delivery	Electronic Delivery	Physical Delivery	Electronic Delivery	
BALLOT DELIVERY	Speed of delivery/ballot replacement	Low	High	Low	High	Low	High	High
	Provide correct ballots	Medium	Medium	Medium	Medium	Medium	Medium	Medium
	Prevent ballot tampering	Medium	High	Medium	High	Medium	High	High
	Prevent ballot spoofing	High	High	High	High	High	High	High
	Ensure proper delivery	Low	High	Low	High	Low	High	High
BALLOT RETURN	Eligibility	Low	Low	Low	Medium	Low	Medium	High
	Privacy	Medium	Medium	Low	Low	Low	Low	High
	Integrity	Low	Low	Low	Low	Low	Low	High
	Voter verifiability - cast as intended	Low	Low	Low	Low	Low	Low	High
	Voter verifiability - counted as cast	Medium	Medium	Medium	Medium	Medium	Medium	High
	Prevent intermediate results	Medium	Medium	Low	Low	Low	Low	High
	Ballot box accuracy	Medium	Medium	Medium	Medium	Low	Low	High
	Coercion and vote buying resistance	Low	Low	Low	Low	Low	Low	Medium
	Channel reliability	Low	Low	High	High	Medium	Medium	High
Auditability	Low	Low	Low	Low	Low	Low	High	

## Appendix A.2: Accessibility assessment table

Requirement	Postal Return		Fax Return		Email return		Secure Electronic Return
	Physical Delivery	Electronic Delivery	Physical Delivery	Electronic Delivery	Physical Delivery	Electronic Delivery	
Blindness	Low	Medium	Low	Medium	Low	High	High
Partial visual loss / visual dysfunction	Medium	Medium	Medium	Medium	Medium	High	High
Deafness	High	High	High	High	High	High	High
Partial hearing loss / tinnitus	High	High	High	High	High	High	High
Dexterity (amputation/loss of limb of upper extremities)	Low	Medium	Low	Medium	Low	High	High
Mobility (amputation/loss of limb of lower extremities)	High	High	High	High	High	High	High
Cognition (behavioral health / TBI)	Medium	Medium	Medium	Medium	Medium	Medium	High