The Council of State Governments

Electronic Ballot Return for Military and Overseas Voters: Considerations for Achieving Balance Between Security and Ballot Access

The electronic return of voted ballots allows military and overseas voters to participate in elections where they would otherwise be unable. Electronic return, as defined here, is the return of a voted ballot via electronic means including email, web portal or fax. The latter of which "can be sent over physical fax machines, through traditional phone lines, digital lines, online services and websites, or mobile phone applications."[1] Electronic return poses unique advantages to military and overseas voters via its ability to serve highly mobile citizens and/or those in highly austere environments. This is a complex issue that requires balance between accessibility, security, and a level of acceptable risk.

Since 2013, the Overseas Voting Initiative (OVI), a collaborative effort between The Council of State Governments (CSG) and the U.S. Department of Defense Federal Voting Assistance Program (FVAP), and in conjunction with our Working Group of state and local election officials, has been committed to ensuring election access for military and overseas citizen voters. The Working Group is uniquely positioned to provide expertise and resources on electronic ballot return as it applies to this group of voters.[2]

Given the sweeping changes necessitated by the COVID-19 pandemic and global mail disruptions, and a new wave of legislation and litigation requiring states to provide increased access to various subsets of voters, now is a good time for a fresh and robust evaluation of the many facets of electronic ballot return.[3]

Any method of returning ballots should be evaluated on a sliding scale, striving to balance access to the ballot with security of the transmission method. There are circumstances in which a military or overseas voter would have no access to return their ballot, except by returning it electronically. Consider the following examples:

---

[1] The Turnout, 2019 (Jared Marcotte, R. Michael Alvarez, PhD, Michelle Shafer): https://turnout.rocks/documents/1/uocava_ballot_return_technical_recommendations_3ULmxP6.pdf

[2] https://ovi.csg.org/wp-content/uploads/2020/03/2019-Examining-Sustainability-of-Balloting-Solutions.pdf

[3] https://ovi.csg.org/wp-content/uploads/2020/07/FailSafeRecommendations.pdf

- Seaman Smith is on a 6-month deployment to the Persian Gulf aboard the destroyer USS Stout. Mail comes by chopper every two weeks, which may delay Seaman Smith from receiving her ballot and potentially condense Smith's opportunity to return her ballot by mail.
- Sergeant James is stationed at a forward operating base in the Middle East. Limited Internet bandwidth is accessible for use on his personal computer, but he does not have access to a printer, scanner, or fax machine to complete the ballot return processes required by some states.
- Dr. Rogers is providing health care in a small, remote area in South America. Mail runs very infrequently, and she lacks access to basic infrastructure, much less internet. On runs into a nearby town for supplies, she sometimes finds internet access, but at speeds much too slow to download an attachment.

Election officials want to provide every single voter with the opportunity to cast a ballot. These officials would benefit from detailed assessments of how to balance the needs of a voter like those above with the security implications of different methods of return.

Although electronic return presents unique risks, there are strategies for reducing some of the risks.[4] Acknowledging that ensuring accessibility and security are foundational to the successful implementation of any voting solution, the OVI recommends the following actions to further develop existing literature and discourse pertaining to electronic ballot return methods in the states:

- Academics and researchers who study election administration and technology should consider:
    - involving state and local election officials in the development of any research on issues and risk mitigations for electronic ballot return options. Electronic ballot return security risks and mitigation strategies are not solely about technology and cybersecurity considerations. They involve people, processes and technology. Those people include election officials. OVI staff and the dedicated election officials comprising the OVI Sustainability of UOCAVA Balloting Systems Working Group are available to assist and provide resources to research efforts.

[4] The Turnout, 2019 (Jared Marcotte, R. Michael Alvarez, PhD, Michelle Shafer) https://turnout.rocks/documents/1/uocava_ballot_return_technical_recommendations_3ULmxP6.pdf

- forming a collaborative group of experts to conduct a comparative risk analysis of *all* ballot return methods, electronic and non-electronic. This study should include research on both analog and digital fax risk mitigation strategies, as well as security mitigations for email, online portals, mobile voting, and other potential technology solutions for ballot transmission. Instead of evaluating one return method in a vacuum, the intent should be to provide a resource that comprehensively compares the benefits and risks of all return methods so states and local jurisdictions can make informed decisions on their usage for their voters. Voters can also use this analysis to weigh the risks of each return method and decide the method most suited to their circumstances. Research into this subject could be extended to other communities that experience similar issues accessing the ballot, such as voters with disabilities, voters living on Native American reservations, and voters with geographical barriers to the ballot.

- Election officials should consider:
  - ensuring their Information Technology (IT) departments or parent IT agencies (e.g., state CIO office) reduce overall cyber risks to elections infrastructure by following the guidance in the National Institute of Standards and Technology (NIST) Cybersecurity Framework. NIST published a draft of an Election Infrastructure Profile to be included in the Cybersecurity Framework to direct current state cybersecurity activities.
  - consulting with the following resources outlining key risk mitigation strategies:
    - NIST
      - Security Best Practices for the Electronic Transmission of Election Materials for UOCAVA Voters[5]
      - Information System Security Best Practices for UOCAVA Supporting Systems[6]
      - NIST Activities on UOCAVA Voting[7]

[5] https://www.nist.gov/system/files/documents/itl/vote/nistir7711-Sept2011.pdf
[6] https://www.nist.gov/system/files/documents/itl/vote/NISTIR-7682-Sept2011.pdf
[7] https://www.nist.gov/uocava-voting

        - The Turnout
            - UOCAVA Electronic Ballot Transmission: Recommendations to Mitigate Security Risks[8]

- State legislators should consider:
    - including election practitioners in policy discussions on expanding electronic ballot return opportunities to certain voters. It is these experts involved in the day-to-day work of serving voters who are best positioned to advise on the complexities of balancing accessibility, security, and a level of acceptable risk.
- The U.S. Election Assistance Commission (EAC) should consider:
    - providing resources in the form of grants and technical assistance for states to adopt risk mitigation strategies and harden systems based on the NIST Cybersecurity Framework.
- Federal agencies such as the Federal Voting Assistance Program (FVAP) and the Department of Homeland Security's Cybersecurity & Infrastructure Security Agency (CISA) should consider:
    - exploring a range of options for secure and efficient electronic communication surrounding the voting process including the transmission of blank and voted ballots for military and U.S. citizens overseas who are covered by UOCAVA without requiring them to find increasingly sparse fax machines. One possible option that could be evaluated for this purpose is the Department of Defense Safe Access File Exchange (DOD SAFE), a secure system used to transfer files across the U.S. Department of Defense. [9] Additionally, ongoing efforts to create secure, encrypted communication platforms should be monitored to determine if any are a viable replacement for current technology.

[8] https://turnout.rocks/documents/1/uocava_ballot_return_technical_recommendations_3ULmxP6.pdf
[9] https://safe.apps.mil/

The OVI studies a subset of voters who are among the most challenging for election officials to serve. Mail has been the primary method of return for military and overseas voters for a century. However, recent disruptions in mail delivery due to a global pandemic, threats of withdrawal from the Universal Postal Union, and UOCAVA voters' austere living situations have demonstrated the vulnerabilities of depending entirely on this method of ballot return. Election officials want to serve each and every voter, and in some cases, a voter may be best served by returning their ballot electronically.

Acknowledging the security vulnerabilities of any method of electronic transmission, states should invest in comparing these methods to traditional, non-electronic ballot return methods with the intent of better meeting their voters' needs. The OVI staff and Working Group of state and local election officials are willing to bring our experience to bear to assist these evaluations in any way possible.