
WEST VIRGINIA CODE CHAPTER 3
ARTICLE 3B

WV Legislature

§3-3B-1. Short title.

This article shall be known as the "Uniformed Services and Overseas Voter Pilot Program."

WV Legislature

§3-3B-2. Uniformed services members and overseas voter pilot program.

This article authorizes a pilot program that will allow counties that meet the minimum requirements contained in section four to use available voting technology for the purposes of voting by absent uniformed services members and overseas citizens, as defined by 42 U.S.C. §1973ff, et seq. Participation in the pilot program will assist counties and the state in identifying areas for potential modification as larger pilot programs of this type begin to be authorized by the federal government under the Military and Overseas Voter Empowerment Act Pub. L. No. 111-84 (2009). Pilot programs authorized by this article are only applicable to the primary and general elections to be held during the year 2010.

§3-3B-3. Process for selection by Secretary of State.

(a) On or before the close of business on January 8, 2010, for the 2010 primary and general election, and on or before the close of business on July 30, 2010, for the 2010 general election only, any county interested in participating in the pilot program must submit a proposal to the Secretary of State. The proposal shall include:

(1) The name of the vendor or vendors, if any, whose voting system will be implemented for voting by uniformed military and overseas citizen voters;

(2) The anticipated cost to the county of implementing the proposal;

(3) The manner in which the voting system complies with the provisions of section four of this article; and

(4) An option for the voter to choose not to vote using the pilot voting system, but rather by mail, fax or e-mail at the voter's discretion as provided in sections five and five-b, article three, chapter three of this code.

(b) The Secretary of State shall evaluate each proposal and shall approve those proposals which meet the criteria described in section four of this article.

(c) On or before January 29, 2010, for the 2010 primary and general election, and on or before August 13, 2010, for the 2010 general election only, each county that has submitted a proposal shall be notified by the Secretary of State that the application has either been approved or denied.

(d) Any county that applied by January 8, 2010, and was approved by the Secretary of State is considered approved for program participation in both the 2010 primary election and 2010 general election.

(e) Following the primary election, the secretary shall evaluate the functional effectiveness of pilot programs conducted under this article and shall terminate any program that fails to adequately and securely ensure that absent uniformed services voters and overseas voters have their absentee ballots cast and counted in the primary election.

(f) Ninety days following the 2010 primary election and ninety days following the 2010 general election, the secretary shall submit to the Legislature reports on the progress and outcomes of any pilot program conducted under this article, together with recommendations:

(1) For the conduct of additional pilot programs; and

(2) For such other legislation as the secretary determines appropriate.

§3-3B-4. Minimum requirements for pilot program voting systems.

Provisions of sections eight and nine, article four-a, chapter three of this code notwithstanding, a voting system may be approved by the Secretary of State for use in the pilot program authorized by this article if it meets the following minimum requirements:

- (1) Basic Operational Elements of the Online Voting System.
 - (A) System is web-based.
 - (B) System has an intuitive, easy-to-navigate interface.
 - (C) System is localized (in terms of date, time and address formats) to major areas in the world.
 - (D) System can handle five thousand voters over ten days, with likely spikes in use at beginning and end of voting period.
- (2) Accessibility.
 - (A) System interoperates with a wide variety of client-side platforms, including:
 - (i) Microsoft Windows;
 - (ii) MacOS;
 - (iii) Other common operating systems (Linux, etc.);
 - (iv) Internet Explorer version 3 or higher;
 - (v) Firefox version 3 or higher;
 - (vi) Safari version 1 or higher;
 - (vii) Opera version 3 or higher;
 - (viii) Netscape version 3 or higher; and
 - (ix) Chrome version 1 or higher.
 - (B) System does not require use of Java/JavaScripts (or detects whether browser accepts Java/JavaScript and provides alternate interfaces.
 - (C) System detects whether browser accepts images and provides alternate interfaces.
 - (D) System works for users who use screen readers.

- (E) System works for users who access the Internet using a text-only browser.
- (F) System is sensitive to low-bandwidth/slow-modem environment of some users.
- (3) Verification of Voters.
 - (A) System verifies a voter's member number, password and PIN number.
 - (B) System alerts administrator of suspected efforts at fraud (including repeated guesses of passwords, excessive votes from a single PC).
- (4) Secret But Verifiable Ballots. System implements secret balloting, while allowing independent third-party monitors to verify that the ballots counted are the same as the ballots cast.
- (5) Support for Ballot Marking Rules. System either:
 - (A) Does not allow mismarking of ballots; or
 - (B) Checks validity of ballots immediately upon submission, and returns ballot to voter for resubmission if there is an error.
- (6) Data Security.
 - (A) System protects the security, integrity, and confidentiality of members' personal data.
 - (B) System protects the security, integrity, and confidentiality of ballots.
 - (C) Ideally, system provides no way for anyone (even vendor employees) to determine how an individual voter voted; at a minimum, system provides reasonable safeguards to prevent such data access.
- (7) Verifiability of Software and Procedures.
 - (A) System and vendor make it possible to verify that the software performs according to specification.
 - (B) System and vendor make it possible to verify that the vendor is running the software correctly.
 - (C) Vendor will allow independent third-party monitors to review:
 - (i) Software, before and during election; and
 - (ii) Procedures (how many people have access to what parts of the system, how passwords are issued, how backups are done).

(D) System incorporates safeguards to assure that vendor employees do not cast votes for users who do not vote.

(E) System provides mechanism for verifying that the system is operating the way it is supposed to; this may involve mathematical procedures or cryptographic protocols that will reveal if ballots have been tampered with, audit trails, or other mechanisms suggested by the vendor.

(F) System automatically verifies the number of ballots sent in and the size and consistency of the database(s), and warns the administrator and stops the voting until the administrator manually authorizes it to continue.

(8) Vendor Transparency and Openness.

(A) Vendor will be sufficiently transparent and open about the system's design and function so as to foster confidence among users.

(B) Vendor will allow independent third-party monitors to verify that the voting system is working according to the specification and proposal.

(9) Vendor Capability.

(A) Vendor is committed to the success of the voting system.

(B) Vendor provides access to 24-hour technical support during the 10-day voting period.

(C) Vendor has tested its voting systems in a production environment.

(D) Vendor will test the voting system prior to the election.

(E) Vendor has, and provides reference for, prior experience with similar systems.