Wisconsin Election Integrity
Promoting our right to self-government through fair & secure elections
WisconsinElectionIntegrity.org

WEC's Security Plan ***degrades*** voting-machine system security.

WEC ignores Wisconsin's most critical missing safeguard (outcome-securing audits); promotes purchase of ballot-marking computers so dangerous they are illegal.

February 25, 2020
Contact: Karen McKim, Coordinator - kmk@wisconsinelectionintegrity.org

The Wisconsin Elections Commission continues to focus security efforts only on its voter-registration system while ignoring dangerous security flaws affecting the voting-machine system. Meeting materials for three security-related agenda items to be discussed at their February 27 meeting contain not a word about, or a penny for, the most gaping hole in Wisconsin's election security: The absence of outcome-securing election audits.

Election-securing audits: The Commission's plan does nothing to address the one and only missing safeguard that causes Wisconsin to rank low on national surveys of states' election security: Election officials in this state do not now and never have performed audits designed to detect and correct hacked election outcomes. Along with paper ballots, these outcome-securing audits are the only voting-system security measure that national experts unanimously identify as essential.

Designed only to detect but not to correct miscounted election results, Wisconsin's occasional random voting-machine audits are more likely to attract than to deter hackers who are bent only on creating chaos. By ignoring this most critical security measure, the Commission is leaving Wisconsin with outdated 20th-century practices while their counterparts in other states move to modern audit methods.

Unverifiable, unauditable, and illegal ballot-marking devices: The Commission's weak vision extends to its apparent ignorance of the risks of universal ballot-marking devices. While ballot-marking devices are necessary for voters with certain disabilities, their universal use impairs election security. When large numbers of voters put down their pens to let computers mark their ballots, the machines become more attractive hacking targets. And because election officials cannot watch over voters' shoulders, voters bear exclusive responsibility for detecting misprinting machines, while auditors and recounters have no way to verify whether the machines correctly recorded voters' selections. The worst kind of BMD prints ballots that encode the votes, so that voters cannot read even the votes printed on their own ballots.

These machines are so dangerous to election security they have been specifically outlawed in at least one other state; they are facing lawsuits in others; and they would be prohibited by pending federal legislation. WEC should never have certified them here because Wisconsin law, too, requires that voters must be able to verify their own votes. Yet rather than move to decertify these dangerous machines, the WEC plan plans to provide security funding to promote their purchase.

Malicious actors already know about these flaws in Wisconsin's voting-machine security.

Wisconsin media's thoughtful accurate coverage of them is the only thing that will motivate officials to correct them.