SHAE SORTWELL

STATE REPRESENTATIVE • 2nd ASSEMBLY DISTRICT

Hearing Testimony
Assembly Committee on Campaigns and Elections
June 6, 2023
Assembly Bill 299

Chairman Krug and members of the Assembly Committee on Campaigns and Elections – thank you for giving me the opportunity to speak on AB 299, relating to requiring identification of a military voter for voting absentee.

AB 299 was crafted to address the military absentee ballot incident from the Milwaukee Elections Commission last fall. This situation showed the system to request military absentee ballots is flawed, and this legislation seeks to solve that problem to ensure security in our election process.

Under this bill, a military voter must provide their federal Department of Defense (DOD) number on the application for an absentee ballot. A municipal clerk must then verify the number with Wisconsin's Department of Military Affairs (DMA), which would obtain that information from the federal government. To ensure a ballot gets to the clerk on time, a military voter may send their ballot through their DOD email to the clerk's office within 30 days of the election.

If a clerk receives a military ballot via regular mail or in-person absentee, they have 48 hours to verify the DOD number. If they receive it via electronic mail, they have up to 90 days after the election to verify it.

If the clerk is unable to verify the DOD number before Election Day, the ballot is considered a provisional ballot. If the clerk is unable to verify the number before 4 p.m. on the Friday following the election, the ballot will not be counted, but the clerk will continue their efforts to verify the voter's DOD number so the voter may use that number to vote at subsequent elections. In utilizing a secure US government email system, clerks should be able to verify the identity of the military personnel more efficiently.

Once verified, a military voter does not need to have their DOD number verified for six years, reducing the administrative work of the municipal clerk and DMA over time.

I want to thank the committee for your time and consideration. I am happy to answer any questions members of the committee may have.

12

ROCK COUNTY, WISCONSIN
Office of the Rock County Clerk
51 South Main Street
Janesville, WI 53545

Lisa Tollefson, Rock County Clerk

Office (608) 757-5660
Fax (608) 757-5662
www.co.rock.wi.us
Lisa.Tollefson@co.rock.wi.us

June 9, 2023

Assembly Committee on Campaigns and Elections Chair and Members:

Testimony for Public Hearing

Chair Krug and Committee Members:

Thank you of allowing testimony today.

Assembly Bill 299 – *Relating to: requiring identification of a military voter for voting absentee.*

- **Against as written**
- When reading this bill, I believe I understand the thought process in attempting to solve a problem. I do have concerns, that it may do more harm than good.

  This bill would require clerks to verify that someone is a *military voter* using the voter's Department of Defense number.

  What if the military will not verify the Department of Defense number?
  - Then will none of our military voters would be allowed to vote.

  What if the military voters does not have a Department of Defense number?
  - In our statures military voter include:
    - A member of the U.S. Army, Navy, Air Force, Marine Corps or Coast Guard, the Commissioned Corps of the Federal Public Health Service or the Commissioned Corps of the National Oceanic and Atmospheric Administration
    - A member of the merchant marine of the United States
    - A civilian employee of the United States and civilians officially attached to the uniformed services who are serving outside the United States
    - A Peace Corps volunteer
    - A spouse or dependent of someone listed above, if you live with or accompany them.
  - It is possible a *military voter* will not have a department of defense number.

  This bill does have an intriguing piece - Returning a military absentee ballot by electronic means. Currently in Wisconsin all ballots must be returned by mail. No one can return a ballot electronically. Other states do have this option for military voters. As a town clerk, I would send out my military ballots as soon as possible. There was one military voter, whose ballot always came back two weeks after the election. Now, many our military voters are having their ballots emailed to them or they pull their ballot from the MyVote system. Which saves on the turn-a-round time for the ballots. But military voters could be called up an anytime, I think this is something we should figure out for our those protecting our country. The first federal ballots for the presidential preference will be sent by February 16, 2024.

Assembly Bill 298 – *Relating to: polling place closures.*

- **Informational**
- The need to have the public's input is important in setting polling locations. This bill does not seem to address special elections or natural disasters.

Assembly Bill 283– *Relating to: aids to counties and municipalities for certain special election costs and making an appropriation.*

- **Support**
- This bill adds consistency to our state statutes concerning who pays for the cost of a special election. If a school district, a county or a city calls for a special election, the entity who calls for a special election pays for elections. This bill follows that same rule. If the state calls for the special election the state pays for the special elections.

Assembly Bill 282– *Relating to: broadcasting election night proceedings.*

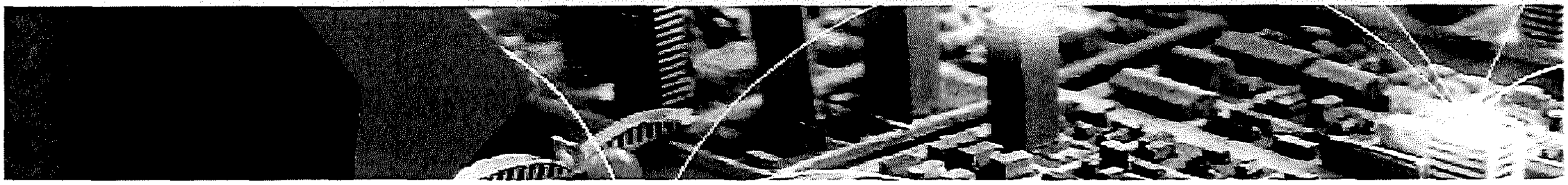
- **Support**
- *This bill requires that if a municipality broadcasts canvass proceedings, then the clerk retains the recordings for 22 months. Retaining a recording of a live broadcast, will help protect our clerks. Over the past few years, we have seen a number of individuals try to put out their own interpretation of events pertaining to elections. An individual could edit a video to show an inaccurate recounting of events. It would be to the clerk's advantage to have the entire recording showing the actual events and the integrity our elections.*

Thank you for your consideration,

Lisa Tollefson
Rock County Clerk

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

39



RISK MANAGEMENT FOR ELECTRONIC BALLOT DELIVERY, MARKING, AND RETURN

INTRODUCTION

Some voters face challenges voting in-person and by mail. State and local election officials in many states use email, fax, web portals, and/or web-based applications to facilitate voting remotely for groups like military and overseas voters and voters with specific needs.

The Cybersecurity and Infrastructure Security Agency (CISA), the Election Assistance Commission (EAC), the Federal Bureau of Investigation (FBI), and the National Institute of Standards and Technology (NIST) assess that the risks vary for electronic ballot delivery, marking, and return. While there are effective risk management controls to enable electronic ballot delivery and marking, we recommend paper ballot return as electronic ballot return technologies are high-risk even with controls in place. Recognizing that some election officials are mandated by state law to employ this high-risk process, its use should be limited to voters who have no other means to return their ballot and have it counted. Notably, we assess that electronic delivery of ballots to voters for return by mail is less vulnerable to systemic disruption.

In this document, we identify risks and considerations for election administrators seeking to use electronic ballot delivery, electronic ballot marking, and/or electronic return of marked ballots. The cybersecurity characteristics of these remote voting solutions are further explored in NISTIR 7551: A Threat Analysis on UOCAVA Voting Systems.

RISK OVERVIEW

	ELECTRONIC BALLOT DELIVERY	ELECTRONIC BALLOT MARKING	ELECTRONIC BALLOT RETURN
Technology Overview	Digital copy of blank ballot provided to voter	Making voter selections on digital ballot through the electronic interface	Electronic transmission of voted ballot
Risk Assessment	Low	Moderate	High
Identified Risks	Electronic ballot delivery faces security risks to the integrity and availability of a single voter's unmarked ballot	Electronic ballot marking faces security risks to the integrity and availability of a single voter's ballot	Electronic ballot return faces significant security risks to the confidentiality, integrity, and availability of voted ballots. These risks can ultimately affect the tabulation and results and, can occur at scale

process, and emails can also be forged to appear as if they were sent from a different address. Furthermore, email is often used in cyberattacks on organizations, such as attackers sending messages with malicious links or attachments to infect computers with malware. This malware could spread to other machines on the network if strong network segmentation techniques are not used.

- Use a dedicated computer that is separated from the remainder of the election infrastructure to receive and process these ballots. For very small offices that may not have the resources to use a dedicated computer, a virtual machine should be installed to separate these devices.
- Patch and configure the computer—as well as document viewer software—against known vulnerabilities (e.g., disable active content, including JavaScript and macros.).
- If possible, implement the .gov top-level domain (TLD). The .gov TLD was established to identify U.S.-based government organizations on the internet.
- Use encryption where possible (e.g., implement STARTTLS on your email servers to create a secure connection, encrypt attached files, etc.)
- Implement Domain-based Message Authentication, Reporting and Conformance (DMARC) to help identify phishing emails.
- Implement DMARC, DomainKeys Identified Mail (DKIM), and Sender Policy Framework (SPF) on emails to help authenticate emails sent to voters.
- Utilize anti-malware detection and encourage voters to as well. Make sure to update the anti-malware regularly.
- Implement multi-factor authentication (MFA) on any email system used by election officials.
- Follow best practices for generating and protecting passwords and other authentication credentials.
- Use a dedicated, shared email address for receiving ballots, such as Ballots@County.Gov. Implement naming conventions in subject lines that will help identify emails as legitimate (e.g., 2020 Presidential General). While a dedicated, shared email account is typically not a best practice, in this instance, it segregates potentially malicious attachments from the network.

WEB-BASED PORTALS, FILE SERVERS, AND APPLICATIONS

Websites may provide accessible and user-friendly methods for transmitting ballots and other election data. While web applications support stronger security mechanisms than email, they are still vulnerable to cyberattacks. Software vulnerabilities in web applications could allow attackers to modify, read, or delete sensitive information, or to gain access to other systems in the elections infrastructure. Sites that receive public input, such as web forms or uploaded files, may be particularly vulnerable to such attacks and should be used only after careful consideration of the risks, mitigations, and security/software engineering practices that went into that software.

- Avoid using knowledge-based authentication (e.g., address, driver's license number, social security number). To the extent practical, implement MFA for employees and voters and mandate MFA for all system administrators and other technical staff (including contractors).
- Patch and configure computers as well as document viewer software against known vulnerabilities (i.e., disable active content, including JavaScript and macros.).

APPENDIX: DETAILED RISK MAPPING

TECHNOLOGY	ELECTRONIC BALLOT DELIVERY	ELECTRONIC BALLOT MARKING	ELECTRONIC BALLOT RETURN
RISK: Exploitation of software flaws in election infrastructure			
Fax	Low	N/A	N/A
Email	Moderate	Moderate	High
Web	High	High	High
RISK: Unauthorized modification(s) to blank ballots			
Fax	Low	N/A	N/A
Email	Moderate	Moderate	N/A
Web	Low	Moderate	N/A
RISK: Loss of voted ballot integrity			
Fax	N/A	N/A	High
Email	N/A	N/A	High
Web	N/A	N/A	High
Risk: Loss of ballot secrecy			
Fax	N/A	N/A	Moderate
Email	N/A	N/A	High
Web	N/A	N/A	High
RISK: Unauthorized individual participates in voting channel			
Fax	Moderate	N/A	High
Email	Low	Low	High
Web	Low	Moderate	High

State of Wisconsin / DEPARTMENT OF MILITARY AFFAIRS

PO BOX 14587
MADISON 53708

TELEPHONE 608 242-3072

Testimony on 2023 Assembly Bill 299

Major General Paul Knapp, The Adjutant General

Assembly Committee on Campaigns and Elections

June 6, 2023

The Department of Military Affairs (DMA) is providing the following in opposition to Assembly Bill 299. This bill requires a military voter to provide his or her federal Department of Defense (DoD) number on the application for an absentee ballot and requires the municipal clerk to verify with the state Department of Military Affairs that the DoD number conforms to the voter's name on the application.

As outlined by Washington Headquarters Services, which is the designated support and service provider of human resources for the military departments, DoD ID Numbers are intended to be known by the individual to whom it belongs and are printed on DoD identification cards. This number is used for individual access to systems, on forms, in digital signatures and for other uses typical of physical and technical identification processes.

Personally identifiable information (PII) is defined by the Department of Defense as information that can be used to distinguish or trace an individual's identity. Additionally, the definition of a record and system of records under the Privacy Act makes it clear that any "identifying number assigned to the individual", triggers provisions of the Privacy Act if the record is retrieved using a unique identifier.

In support of the definitions above, Department of Defense policy classifies DoD numbers as personal identifiable information (PII), and as such cannot be used for any purpose outside of DoD approved instances. The policy clearly states that the DoD ID Number shall only be used for DoD business purposes, and but may include transactions with entities outside DoD, so long as individuals are acting on behalf of or in support of the DoD. This proposed legislation would violate PII regulations, DoD policy and provisions of the Privacy Act, and would not allow for the Wisconsin Department of Military Affairs to provide individual DoD ID numbers to municipal clerks.

Additionally, this bill insinuates that the Wisconsin Department of Military Affairs holds the DoD ID numbers for all branches of the armed services, which is incorrect. Service members from all branches of service are eligible voters in Wisconsin and are in an array of statuses to include Active Duty, National Guard and Reserve. The Wisconsin Department of Military Affairs does not have access to or house DoD ID numbers for all service members across all branches, but only for Wisconsin National Guard members.

For all of the reasons above, we are unable to provide support for Assembly Bill 299 and respectfully request that Assembly Bill 299 is not pursued as written.

Wisconsin Democracy Campaign

203 South Paterson Street, Suite 100 / Madison, WI 53703-3689 / 608 255-4260 / www.wisdc.org

Testimony of Matt Rothschild,
Executive Director, Wisconsin Democracy Campaign
To the Assembly Committee on Campaigns and Elections
Re: Assembly Bill 299
June 6, 2023

Chair Krug, and other distinguished members of this committee,

Good morning, I'm Matt Rothschild, the executive director of the Wisconsin Democracy Campaign, which, since 1995, has been tracking and exposing the money in Wisconsin politics, and we've also been advocating for a broad range of pro-democracy reforms.

We oppose Assembly Bill 299.

First, we see this as part of an effort that has been under way here in Wisconsin since 2011 to make voting more difficult and to make the people of Wisconsin suspicious about the validity of our voting systems and the reliability of our election results. None of that is healthy for our democracy.

Second, **the simple fact is that this bill would make it harder for service members to vote.**

Under current law, service members aren't required to provide ID proof when applying for an absentee ballot. Now they'd have to, and it wouldn't be easy. This bill would require service members to jump through several hoops before they could get their absentee ballot.

The member would have to provide their federal DOD number on the application.

Then the municipal clerk would have to verify that number with the Department of Military Affairs.

SECURE
DEMOCRACY
USA

Chair Krug, Vice-Chair Maxey, and honorable members of the committee,

Thank you for the opportunity to submit testimony on Assembly Bill 299.

Secure Democracy USA is a nonpartisan, nonprofit organization that works to build confidence in our elections and improve voter access across the United States. We educate policymakers and the public about what it takes to safeguard our voting systems.

Americans serving in the armed forces, and their families, rightfully have special consideration in the laws governing voting access under the Uniformed and Overseas Citizen Absentee Act (UOCAVA). Servicemembers make unique commitments to their country, commitments which should be coupled with a unique commitment by the government to ensure their freedoms as voters are respected in spite of the logistical challenges of deployment abroad.

AB 299 appears to intend to allow electronic ballot return for UOCAVA voters. This change would be an improvement for voters, bringing Wisconsin in-line with the best practices from most states. 26 states, including Indiana, Iowa, and Missouri, allow UOCAVA voters to return a ballot by secure email. However, as drafted, AB 299 does not amend all of the sections of code that must be amended to authorize electronic ballot return; the bill would need to also amend sections § 6.87(3)(d) or (4)(b)(1).

As currently drafted, AB 299 could present new challenges for UOCAVA voters. UOCAVA exempts members of the military, their dependents, and overseas voters from providing photo ID for federal elections. This exemption carries through Wisconsin law for all elections. The purpose of this exemption is to make the process for registration and voting easier on this population. This bill effectively establishes an ID requirement for military service members and their dependents, creating an obstacle for them to have their vote counted. Additionally, this bill would not permit military voters to cure their absentee ballot, potentially disenfranchising servicemembers for small, innocent mistakes.

AB 299 also poses potentially impossible administrative challenges for election administrators. The bill would require municipal clerks to verify the military service members through the Wisconsin Department of Military Affairs branch by the Friday after the election. If the clerk is unable to verify this information, the ballot will not be counted. Last year Michigan passed similar legislation, but appears to have been unable to implement the legislation due to the challenges of protecting personally identifiable information from the Common Access Cards.

We would welcome further engagement with the bill authors to discuss these outstanding questions.

Respectfully submitted,

Evan Preston
Director of Advocacy, Secure Democracy USA

Secure Democracy USA is a nonpartisan, nonprofit 501(c)(4) organization that works to build confidence in our elections and improve voter access across the United States. We educate policymakers and the public about what it takes to safeguard our voting systems. We use survey and messaging research to inform our strategy and we collaborate with state leaders, election administrators, policy experts, and allies to ensure that all eligible citizens have the freedom to vote how they choose.