LEAGUE OF WOMEN VOTERS® OF MASSACHUSETTS
133 Portland Street, Boston, MA 02114 • Tel: 617-523-2999 • Fax: 617-248-0881
E Mail: lwvma@lwvma.org • Website: www.lwvma.org

Testimony in opposition to
H.2102 An Act relative to UOCAVA voting
Submitted to the Joint Committee on Election Laws
By Linda Freedman, LWVMA Election and Voting Specialist
October 12, 2017

The League of Women Voters is dedicated to improving voter participation and supports accessibility to the polls and equal treatment of voters, but not at the expense of security, accuracy and secrecy of the ballot. The League opposes H.2102, which allows uniformed and overseas citizens to receive and send their ballots by internet, a secure website or fax. The League only supports voting systems and procedures that are secure, accurate, recountable, accessible and transparent. The League currently opposes internet voting because it is insecure and the accuracy cannot be verified by the voter. At this time, there are no reliable methods to prevent interception of electronic ballots which can be altered and received as legal votes by unsuspecting local election offices. Overseas voters would not see any changes that might be made to their ballot.

The counsel for the Secretary of State has failed to define "a secure website" or require continuous protection and testing for it. There is ample evidence of secure websites that have been penetrated and valuable data stolen. This includes massive data theft from government, defense contractors, banks, corporations, merchants and Equifax, a major supplier of credit information for 140 million people. Local election offices as well as overseas ballots would be at risk with electronic ballots.

Voting by email and fax is extremely insecure. Electronic ballots are targets for cyber thieves who can change the outcome of an election by altering the votes. Undisclosed domestic campaign funds could finance this, as could foreign governments and agencies. Electronic ballots are also vulnerable to vote buying or intimidation. The overseas voters must waive their right to a secret ballot when using electronic transmission.

Recently, the chairs of the US Senate Intelligence committee warned all election officials about future cyber security attacks by Russians. Senator Richard Burr of North Carolina said, "The Russian intelligence service is determined—clever—and I recommend that every campaign and every election official take this very seriously."

The Department of Defense, the National Institute of Standards and Technology and senior cyber security officials at the Department of Homeland Security previously opposed returning ballots electronically because those ballots are too insecure for transmission. The Department of Defense warned that it cannot ensure the legitimacy of ballots sent over the internet and has stated ***"[the Department of Defense] does not advocate for the electronic transmission of any voted ballot, whether it be by fax, email or via the Internet."***[i] In addition, the Department of Defense's Federal Voting Assistance Program, in a report to Congress in 2013, stated clearly that the postal mail return of a voted ballot, coupled with the electronic

transmission of a blank ballot is the "most responsible"[ii] method of absentee voting for uniformed and overseas voters. The overwhelming evidence that secure internet voting is not within our grasp led Congress to repeal a directive to the Department of Defense to pursue online voting for military and overseas voters in the 2015 National Defense Authorization Act.

We strongly urge you to block passage of this bill. Thank you for your consideration.

---

[i] Pentagon spokesman Lt. Commander Nathan Christensen, April 16, 2015
Gordon, Greg, "As states warm to online voting, experts warn of trouble ahead," The Olympian, April 16, 2015

[ii] Federal Voting Assistance Program, May 2013, "2010 Electronic Voting Support Wizard (EVSW) Technology Pilot Program Report to Congress http://www.fvap.gov/uploads/FVAP/Reports/evsw_report.pdf