January 25, 2019

The Honorable Kirk Cox (*via email DelKCox@House.Virginia.gov*)
Speaker of the House

The Honorable S. Chris Jones (*via email DelCJones@House.Virginia.gov*)
Chair, House Appropriations Committee

The Honorable Mark M. Cole (*via email DelMCole@House.Virginia.gov*)
Chair, House Privileges and Election Committee

Pochahontas Building
900 E. Main Street
Richmond, VA 23219

The Honorable Ryan T. McDougle (*via email district04@senate.virginia.gov*)
Chair, Senate Rules Committee

The Honorable Jill Holtzman-Vogel
Chair, Senate Privileges and Election Committee

The Honorable Tommy K. Norment *(via email district03@senate.virginia.gov)*
The Honorable Emmett Hanger *(via email district24@senate.virginia.gov)*
Co-Chairs, of Senate Finance Committee

P.O. Box 396
Richmond, VA 23218

RE: Internet Voting

Dear Del. Cox, Del. Jones, Del. Cole, and Sen. McDougle, Sen. Vogel, Sen. Norment, Sen. Hanger,

We write in opposition to HB2588, HJ670, and SJ291, which propose studying and piloting electronic forms of voting for deployed military. Cybersecurity experts agree that internet return of marked ballots lacks sufficient safeguards for security and privacy, and Virginia's own SB 11 workgroup report confirms its vulnerabilities. Verified Voting supports the United States military - our staff members have family members who are currently serving. Because of our respect for those who risk their lives to protect our country, we oppose subjecting our service men and women to a voting system that puts the validity and privacy of their votes at greater risk than their civilian counterparts.

Under current technology, no practically proven method exists to securely, verifiably or privately return voted materials over the internet. Cybersecurity experts agree that no current technology, including blockchain voting, can guarantee the secure, verifiable, and private return of voted ballots over the internet. Both because there could be vote-rigging malware on the voter's

computer and because electronically returned ballots could be intercepted and changed or discarded en route, local elections officials would be unable to verify that the voter's ballot accurately reflects the voter's intent. Furthermore, even if the voter's selections were to arrive intact, the voted ballot could be traceable back to the individual voter, thereby violating Virginia's constitutional protections guaranteeing the right to a secret ballot.

HB 2588, HJ760 and SJ291

All of the pending bills and resolutions require a "secure" method of voting. No such system is commercially available despite the use of insecure internet voting methods in some other states and countries. For Virginia to attempt to develop such a system on its own would be prohibitively expensive. More importantly, it is very unlikely that Virginia would succeed in developing such a system when the Department of Defense and National Institute for Standards and Technology (NIST) spent millions of dollars attempting to do just that and abandoned the program when it became clear that no secure method of voting is available.[1] Specifically, NIST stated:

> The study concluded that Internet voting systems cannot currently be audited with a comparable level of confidence in the audit results as those for polling place systems. Malware on voters' personal computers poses a serious threat that could compromise the secrecy or integrity of voters' ballots. And, the United States currently lacks a public infrastructure for secure electronic voter authentication. Therefore, NIST's research results indicate that additional research and development is needed to overcome these challenges before secure Internet voting will be feasible.

The National Academies of Science, Engineering, and Medicine in 2018 released the report entitled *Securing the Vote: Protecting American Democracy*[2] which gives the following recommendation:

> 5.11 At the present time, the Internet (or any network connected to the Internet) should not be used for the return of marked ballots. Further, Internet voting should not be used in the future until and unless very robust guarantees of security and verifiability are developed and in place, as no known technology guarantees the secrecy, security, and verifiability of a marked ballot transmitted over the Internet.

The report also advised that experts should be consulted. In short, the studies and pilots proposed in these bills go against recommendations, would incur significant costs, and the efforts would be guaranteed to fail to secure our military citizens' votes.

[1] NIST Activities on UOCAVA Voting; http://www.nist.gov/itl/vote/uocava.cfm

[2] National Academies Press https://www.nap.edu/catalog/25120/securing-the-vote-protecting-american-democracy

Internet voting is the most vulnerable method of voting

Anyone in the world, including foreign nation states, criminal organizations, or our domestic partisans, can attack any Internet voting system, attempt to change votes, violate privacy, or disrupt the election - possibly in a completely undetectable way. The kinds of attacks that are credible threats and elevate the risk of voting via the internet include the following:

- Voter authentication attacks (i.e. forged voter credentials)
- Malware on voters' devices (e.g., viruses, Trojan horses, malicious code embedded in software updates) that can modify votes undetectably
- Denial of service attacks (slowing some key part of the system to a crawl, or crashing it, either by overwhelming it with traffic or taking advantage of a bug)
- Server penetration attacks (remote break-in and control of the election server)
- Spoofing attacks (directing voters to a fake voting site instead of the real one)
- Widespread privacy violation (by any of several methods, taking advantage of the fact that online voters must transmit their names with their votes)
- Automated vote buying and selling schemes (with cryptocurrency payments, e.g. Bitcoin, in exchange for votes)

More importantly, the security of the device that voters use to cast their votes is unknowable. The device may already be corrupted with malware or viruses that could interfere with ballot transmission or even spread that malware to the computer at the elections office on the receiving end.

Prevention of attacks is impossible, as are audits

Cyber security experts agree that completely preventing attacks is impossible despite the use of best practices in cybersecurity. Resiliency, namely the capability to recover from an attack or error, is a critical component of cybersecurity protection. With insecure internet voting, no trustworthy record of the voter's choices exists, and therefore it is impossible to perform meaningful audits or recover from an attack or a hack.

Internet voting does not solve the policy issue

The belief that overseas military voters need internet voting is several years out of date. With the advent of the 45-day lead time for mailing absentee ballots, almost all voters anywhere, should be able to receive their ballots, make their choices, and return their ballots within that window. If the problem is late return of ballots, safer policy choices exist to address that problem, e.g. extending the deadline for receipt of voted ballots.

Virginia should not embark on a costly exercise to introduce internet voting that will increase the risk to unacceptable levels for our service men and women. We urge Virginia legislators to responsibly vote against these bills.

Verified Voting is a national, non-profit non-partisan information and advocacy organization focused exclusively on ensuring the security, integrity, and trustworthiness of computerized election technology. We protect the right to vote where voting intersects technology and

advocate for the responsible use of emerging technologies to ensure that Americans can be confident their votes are cast as intended and counted as cast.

Respectfully submitted,

Marian K. Schneider, President
Verified Voting
cc: Members of the Virginia Senate
Members of the Virginia House of Delegates

The following signatories add their names in opposition to the proposed bills. ***Institutional affiliations are provided only for the purpose of identification and do not imply institutional endorsement or approval of this letter.***

Verified Voting Board Members:

Joseph Lorenzo Hall
Chief Technologist, Center for Democracy & Technology

David Jefferson
Computer Scientist, Lawrence Livermore National Laboratory

Ronald L. Rivest
MIT Institute Professor
Member, US National Academies of Sciences, Engineering, and Medicine

Barbara Simons
IBM Research (retired)
Board of Advisors, EAC
Former President, ACM
Board Chair, Verified Voting Board

Verified Voting Advisory Board Members:

Jeffrey Bleich
US Ambassador (ret.)

Cindy Cohn
Executive Director
Electronic Frontier Foundation

Larry Diamond
Senior Fellow, Hoover Institution
Senior Fellow, Center on Democracy, Development & the Rule of Law, Freeman Spogli Institute for International Studies
Stanford University

Jeremy Epstein
Fairfax, VA
Verified Voting Advisory Board

Martin Hellman
Member, US National Academies of Sciences, Engineering, and Medicine
Professor Emeritus of Electrical Engineering, Stanford University

Candice Hoke
Founding Co-Director, Center for Cybersecurity & Privacy Protection
C|M Law, Cleveland State University

Professor Eugene H. Spafford
Director Emeritus, Purdue University CERIAS

Bruce Schneier
Fellow and Lecturer, Harvard Kennedy School