Chair Jack Reed
Ranking Member James Inhofe
Senator Jeanne Shaheen
Senator Kirsten Gillibrand
Senator Richard Blumenthal
Senator Mazie Hirono
Senator Tim Kaine
Senator Angus King
Senator Elizabeth Warren
Senator Gary Peters
Senator Joe Manchin III
Senator Tammy Duckworth
Senator Jacky Rosen
Senator Mark Kelly
Senator Roger F. Wicker
Senator Deb Fischer
Senator Tom Cotton
Senator Mike Rounds
Senator Joni Ernst
Senator Thom Tillis
Senator Dan Sullivan
Senator Kevin Cramer
Senator Rick Scott
Senator Marsha Blackburn
Senator Josh Hawley
Senator Tommy Tuberville
U.S. Senate Committee on Armed Services
Washington, DC 20510

October 13, 2021

Dear Chair Reed, Ranking Member Inhofe, and Members of the Committee,

As specialists in election security, computer science, and election administration, we are writing to express profound opposition to provisions in H.R. 4350, the National Defense Authorization Act for Fiscal Year 2022, as passed in the House of Representatives, that would fund the electronic transmission of voted ballots for absent uniformed service and overseas voters.

We have long supported responsible uses of technology to facilitate voting for voters covered under the Uniformed and Overseas Citizen Absentee Voter Act (UOCAVA), including online voter registration, electronic submission of the FPCA,[1] and electronic blank ballot delivery. But we strongly oppose policies that promote or expand the electronic return of voted ballots because of the serious and unsolved security vulnerabilities. We write to you today to urge the Senate to not include provisions (Sec. 1075 and 1081) currently in HR 4350, that would fund and expand online voting. At a time when election security and

[1] Federal Postcard Application.

public confidence of our elections are under attack, increased electronic return of voted ballots, known as internet voting, is not safe or secure, and will undermine confidence and trust in elections.

Online voting has been rejected as unacceptably insecure by DHS, FBI, NIST, the Senate Select Committee on Intelligence and the National Academies of Science, Engineering and Medicine.

Among computer scientists and national security experts there is no debate: online voting cannot be adequately secured for governmental elections. Last year, the Department of Homeland Security (DHS), the U.S. Election Assistance Commission, the Federal Bureau of Investigation, and the National Institute of Standards and Technology specifically advised **"**we recommend paper ballot return as electronic ballot return technologies are **high-risk even with [risk-management] controls in place**."[2] In other words, the security tools currently available such as end-to-end verifiability, encryption, cloud-based services, and distributed ledger technology (blockchain), are unable to secure online voting systems. The risk assessment went on to warn that electronic ballot return "**creates significant security risks to the confidentiality of ballot and voter data (e.g., voter privacy and ballot secrecy), integrity of the voted ballot, and availability of the system. We view electronic ballot return as high risk. Securing the return of voted ballots via the internet while ensuring ballot integrity and maintaining voter privacy is difficult, if not impossible, at this time**."[3]

DHS's blunt warning against the use of online voting echoed bipartisan recommendations from the Senate Select Committee on Intelligence published in response to findings that foreign governments were actively trying to attack U.S. election systems. The Committee wrote: "States should resist pushes for online voting. One main argument for voting online is to allow members of the military easier access to their fundamental right to vote while deployed. While the Committee agrees states should take great pains to ensure members of the military get to vote for their elected officials, no system of online voting has yet established itself as secure."[4]

In 2018, the National Academies of Sciences, Engineering and Medicine (NASEM) released a report stating that **the technology to return marked ballots securely and anonymously over the internet does not exist**. Many studies have reviewed specific internet voting systems and consistently, all have found that despite their claims of innovation, these systems have fundamental vulnerabilities.

Provisions in HR4350 will not ensure secure online voting.

Perhaps with the intent to address some of these risks, Section 1075 of HR4350 contains language that endorses *end-to-end electronic voting services*. Security researchers have explored *end-to-end verifiable voting systems* which allow voters to verify that their votes were correctly recorded and included in the final totals, and that allow the public to count the recorded votes and check the totals. Section 1075 may intend to require end-to-end verifiability, but in our reading, it does not adequately define this requirement. More important, end-to-end verifiability – albeit an essential requirement of an internet voting system – does not suffice to address the dangers of internet voting.[5] End-to-end verifiability cannot protect against voter authentication attacks (forged credentials), malware on a voter's device, server

[2] Available at: https://epic.org/privacy/voting/Risk-Management-Electronic-Ballot-May2020.pdf
[3] Ibid.
[4] Report of the Select Committee on Intelligence, United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, Volume 1: Russian Efforts Against Election Infrastructure with Additional Views, 2019, Available at https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf

[5] The most comprehensive study of end-to-end verifiable internet voting, *The Future of Voting*, concluded that "many challenges remain in building a usable, reliable, and secure E2E-VIV [End-to-End Verifiable Internet Voting] system," which must be overcome before using internet voting in public elections. It further concluded that internet voting should not be used in public elections until end-to-end verifiable systems have been widely deployed for *in-person* voting. Such systems have been piloted in a few small jurisdictions, but they have not yet been adopted on a wider scale.

penetration, and denial of service (DDOS) attacks – any and all of which would be extremely disruptive for military service members' voting and could potentially compromise military infrastructure.

Limiting the bill's scope to military voters in "locations with limited or immature postal service," as specified in Section 1075, does not justify the initiative. The bill does not define what qualifies as "limited or immature postal service," making it unknown how many military voters would qualify for electronic ballot return. The more widely the system is extended, the greater the threat to the credibility of elections. Although such a system may aim to enfranchise servicemembers, it can be subverted and used to undermine free and fair elections.

Section 1081 seeks to fund a provision in the Military and Overseas Voter Empowerment (MOVE) Act to pilot technology to "improve the security of ballot transmission, including through the use of cloud-based and distributed ledger-based solutions, to enable ballot transmission to meet existing Federal cybersecurity guidelines." As already determined by the DHS, SSCI and NASEM, these security tools cannot solve the risks inherent to internet voting and may instead introduce additional security vulnerabilities. Further, multiple studies have shown how online voting systems with these features can be compromised.[6]

There are solutions to improve military and overseas voting without expanding dangerously insecure voting technology.

We emphatically support interventions to assure that servicemembers have equal opportunity to securely and verifiably cast their votes in U.S. elections. Better options than internet voting exist, often building upon systems already in place:

- Automatic voter registration for eligible members of the military
- Automatic mailing of ballots to registered military
- Broader use of DOD Label 11 for free-of-charge express mail ballot return
- Improved ballot tracking services
- Extending deadlines for the return of military ballots

Voter registration: Only about two-thirds of military members were registered to vote in 2020, a registration rate 14 percentage points lower than that of the general population. Making voter registration automatic for all eligible citizens during the enlistment process would help reduce this gap. Unlike internet voting, this is an achievement that is within reach.

Ballot mailing: Automatically mailing ballots to registered military voters would eliminate the need for service members to re-file yearly for a ballot. (Under UOCAVA, the Uniformed and Overseas Citizens Absentee Voting Act, servicemembers also can opt to receive their blank ballots electronically; electronic delivery of blank ballots does not present the same risks as electronic return of voted ballots.)

Ballot return and tracking: Ballot return should be expedited through the existing DOD Label 11 no-charge taxpayer-funded express ballot return service, and ballot tracking services should be expanded for military and overseas voters – as has already successfully been done in many states.

Extending deadlines: Because UOCAVA requires that ballots be sent or electronically delivered to overseas voters starting 45 days before an election, most voters can receive, mark, and timely return a paper ballot. Ballots from military voters are most likely to be rejected because they were received after the deadline. Many states accept military and overseas ballots that are postmarked before Election Day even if they arrive after Election Day. The bill should require that *all* states extend the deadline for receipt

[6] *See*: Michael A. Spector, J. Alex Halderman, Security Analysis of the Democracy Live Online Voting System," University of Michigan, June 7, 2020. *Available at: https://internetpolicy.mit.edu/wp-content/uploads/2020/06/OmniBallot.pdf*, Michael Spector, James Koppel, Daniel Weitzner, "The Ballot is Busted Before the Blockchain: A Security Analysis of Voatz, the First Internet Voting Application Used in U.S. Federal Elections," Massachusetts Institute of Technology, February 2020, and Trail of Bits Full Report on the Voatz Mobile Voting Platform, *available at:* https://blog.trailofbits.com/2020/03/13/our-full-report-on-the-voatz-mobile-voting-platform/

of returned military/overseas ballots to the latest date practicable before the election must be certified, or a minimum of 7 days, as long as they have been sent by Election Day.

We believe that servicemembers deserve the highest standard of safe and verifiable voting. For the foreseeable future, internet voting cannot meet that standard, and places military voters' votes – and the trustworthiness of elections themselves – at risk. While the federal government may be able to play a constructive role in overcoming the obstacles to secure internet voting, HR4350's requirement of an internet voting implementation plan is recklessly premature.

We recommend a broader, more deliberative approach to identifying and overcoming obstacles to secure and reliable military voting. We would welcome the opportunity to provide further information on technical aspects of end-to-end verification and internet voting and/or other suggestions to improve military voting.

Sincerely,

Common Cause

Protect Democracy

Free Speech For People

U.S. Vote Foundation

Verified Voting

Dr. Andrew W. Appel*
Professor of Computer Science,
Princeton University

Dr. Elizabeth Bradley*
Professor
University of Colorado Boulder

Dr. Duncan Buell*
Chair Emeritus — NCR Chair in Computer Science and Engineering
Dept. of Computer Science and Engineering
University of South Carolina

Dr. Larry Diamond*
Senior Fellow, Hoover Institution and Freeman Spogli Institute,
Stanford University

Dr. David L. Dill*
Donald E. Knuth Professor, Emeritus, in the School of Engineering, Stanford University
Founder of VerifiedVoting.org

Dr. Michael Fischer*
Professor of Computer Science,
Yale University

Dr. J. Alex Halderman*
Professor, Computer Science and Engineering
Director, Center for Computer Security and Society
University of Michigan

Dr. Martin E. Hellman*
Member, US National Academy of Engineering
Professor Emeritus of Electrical Engineering,
Stanford University

Candice Hoke
Founding Co-Director, Center for Cybersecurity & Privacy Protection,
Cleveland-Marshall College of Law, Cleveland State University

Dr. David Jefferson*
Lawrence Livermore National Laboratory
(retired)

Lowell Finley*
Former Deputy Secretary of State
California

Dr. Douglas W. Jones*
Emeritus Associate Professor of Computer Science
University of Iowa

Douglas A. Kellner *
Co-Chair, New York State Board of Elections

Dr. Daniel P. Lopresti*
Professor, Department of Computer Science and Engineering
President, International Association for Pattern Recognition (IAPR)
Vice Chair, Computing Research Association's Computing Community Consortium (CCC)
Lehigh University

Dr. John L. McCarthy*
Computer scientist (retired)
Lawrence Berkeley National Laboratory

Mark Ritchie*
Former MN Secretary of State
Member of the EAC Board of Advisors
Former president of the National Association of Secretaries of State

Dr. Ronald L. Rivest*
Massachusetts Institute of Technology

Paul Rozenzweig*
Professorial Lecturer in Law
George Washington University

Dr. John E. Savage*
An Wang Professor of Computer Science, Brown University

Bruce Schneier*
Fellow and lecturer
Harvard Kennedy School of Government

Kevin Skoglund*
President and Chief Technologist
Citizens for Better Elections

Dr. Barbara Simons*
IBM Research (retired),
former President Association for Computing Machinery (ACM)

Dr. Philip B. Stark*
Professor of Statistics
Associate Dean, Division of Mathematical and Physical Sciences
University of California, Berkeley

Professor Eugene H. Spafford*
Executive Director Emeritus, CERIAS
Purdue University

Dr. Poorvi L. Vora*
Professor of Computer Science
The George Washington University

Dr. Dan Wallach*
Professor, Department of Computer Science
Rice Scholar, Baker Institute for Public Policy
Rice University

*Affiliations listed for identification purposes only and do not imply institutional endorsement.