June 15, 2022

The Honorable Isaac G. Bryan, Chair
The Honorable Kelly Seyarto, Vice Chair
The Honorable Steve Bennett
The Honorable Evan Low
The Honorable Chad Mayes
The Honorable Kevin Mullin
The Honorable Blanco Rubio
California State Assembly Committee on Elections
Legislative Office Building
Room 365
1020 N Street
Sacramento, California

Re: **SB 1480 STRONG OPPOSE**

Dear Chair Bryan, Vice Chair Seyarto and members of the Committee,

As members of the computer science, cybersecurity, and election integrity communities, we are writing to share information on the scientific conclusions regarding the insecurity of Internet voting, and to urge you in the strongest possible terms to vote NO on SB 1480.

SB 1480 (Glazer) would allow voters with disabilities to vote by facsimile, and with today's telephonic networks, that means these ballots will be sent over the Internet. SB 1480 would also permit the Secretary of State to certify an online ballot return system. Sending voted ballots over the Internet, by facsimile, electronic ballot return system, or any other means, creates profound, dangerous, and currently unsolvable security vulnerabilities. Put simply, online voting is unacceptably insecure for public elections–as the National Academies and Federal security agencies agree. There is no technology currently available or expected in the foreseeable future that can adequately secure elections when ballots are faxed or electronically transmitted over the Internet. SB 1480 would exponentially increase the number of ballots that could be transmitted over the Internet, profoundly weakening the security and integrity of California's elections.

At a time when election security and public confidence of our elections are under attack, increased electronic return of voted ballots, whether from a phone, tablet, or computer, is simply not safe or secure, and will erode confidence and trust in elections. Furthermore, with the ongoing conflict in Ukraine, the threat of Russian cyber attacks on our election infrastructure has escalated.[1] Election systems have been recognized as part of our critical infrastructure[2] and must be treated as a national security asset. Now is not the time to be adopting election processes that are known to be vulnerable to hackers.

Federal security agencies have urged States not to adopt online voting.

Online voting has been rejected as unacceptably insecure by the Department of Homeland Security, FBI, and the National Institute of Standards and Technology,[3] the Senate Select Committee on Intelligence[4] and the National Academies of Science, Engineering and Medicine.[5] Among computer scientists, national election security experts and federal security agencies, there is no debate: online voting cannot be adequately secured for governmental elections.

In 2020, 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 issued a risk-assessment to state officials which expressly stated:

> *"…we recommend paper ballot return as electronic ballot return technologies are high-risk even with [risk-management] controls in place."*[6]

---

[1] Joseph Marks, "Russian hacking threats aren't over, Congress was warned last night," *The Washington Post*, March 9, 2022. *Available at: https://www.washingtonpost.com/politics/2022/03/09/russian-hacking-threats-arent-over-congress-was-warned-last-night/*

[2] "The Designation of Election Systems as Critical Infrastructure," Congressional Research Service, September 18, 2019. Available at: https://sgp.fas.org/crs/misc/IF10677.pdf

[3] "Risk Management for Electronic Ballot Delivery and Marking," Cyber Security and Infrastructure Security Agency, Federal Bureau of Investigation, National Institute of Standards and Technology, U.S. Election Assistance Commission. *Available at: https://www.politico.com/f/?id=00000172-9406-dd0c-ab73-fe6e10070001*

[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] National Academies of Science, Engineering, and Medicine, 2018. "Securing the Vote: Protecting American Democracy." Washington, DC: The National Academies Press. *Available at: https://www.nap.edu/catalog/25120/securing-the-vote-protecting-american-democracy*

[6] See *supra* note 3.

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."*[7]

DHS's blunt warning against the use of online voting echoed bipartisan recommendations from the Senate Select Committee on Intelligence issued 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."*[8]

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.[9] Many studies have reviewed specific Internet voting systems, and consistently, all have found that despite their claims of innovation, these systems have fundamental vulnerabilities.[10]

---

[7] Ibid.

[8] See *supra* note 4.

[9] See *supra* note 5.

[10] Michael A. 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, 2020, available at: https://Internetpolicy.mit.edu/wp-content/uploads/2020/02/SecurityAnalysisOfVoatz_Public.pdf ;
Thomas Haines, Olivier Pereira, Vanessa Teague, "Report on theSwiss Post e-voting System," March 24, 2022, available at: https://ieeexplore.ieee.org/document/9152765

We understand the profound challenges you face to assure every voter's ability to vote and strongly support interventions to assure voters' equal opportunity and access to cast their vote – securely and verifiably. Recognizing that no current solution is ideal for all voters, we support thoughtful consideration of other secure innovations, such as improving California's existing Remote Accessible Vote by Mail (RAVBM) options. This solution allows for electronic delivery of a blank ballot to the voter so they may use their own accessible equipment at home to mark their ballot, print it out and return the paper ballot to their election office. However, Internet voting, (with or without blockchain), is not the answer.

We would welcome the opportunity to provide lawmakers with further information on technical aspects of Internet voting. For the present, we urge the California legislature in the strongest possible terms to heed the warnings from our nation's security agencies and computer experts, and to vote NO on SB 1480.

Respectfully submitted,

Andrew W. Appel, Ph.D.
Eugene Higgins Professor of Computer Science
Princeton University*

Duncan Buell, Ph.D.
Chair Emeritus — NCR Chair in Computer Science and Engineering
Department of Computer Science and Engineering
University of South Carolina*

Richard A. DeMillo, Ph.D.
Charlotte B. and Richard C. Warren Professor of Computer Science
College of Computing
Georgia Institute of Technology*

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

Drew Springall, Travis Finkenauer, Zakir Durumeric, Jason Kitcat, Harri Hursti, Margaret MacAlpine, and J. Alex Halderman, "Security Analysis of the Estonian Internet Voting System," November 2014, available at: https://estoniaevoting.org/findings/paper/

Lowell Finley
Former California Deputy Secretary of State for Voting System Technology and Policy (2007-2014)

Michael J. Fischer, Ph.D.
Professor of Computer Science
Yale University*

Susan Greenhalgh
Senior Advisor for Election Security
Free Speech For People

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

David Jefferson, Ph.D.
Lawrence Livermore National Laboratory* (retired)

Douglas W. Jones, Ph.D.
Emeritus Associate Professor of Computer Science
University of Iowa*

Arthur M. Keller, Ph.D.
Former Chair, Voting Systems Standards Committee, Institute for Electrical and Electronic Engineers*

Daniel P. Lopresti, Ph.D.
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*

Peter G. Neumann, Ph.D.
Chief Scientist
SRI International Computer Science Lab*

Ron Rivest, Ph.D.
Institute Professor
Massachusetts Institute of Technology*

Kevin Skoglund
President and Chief Technologist
Citizens for Better Elections*

Eugene H. Spafford, Ph.D.
Professor and Emeritus Executive Director
CERIAS, Purdue University

Philip B. Stark, Ph.D.
Distinguished Professor of Statistics
University of California, Berkeley*

Phillip J. Windley, Ph.D.
Former State CIO, State of Utah
Founding Chair, Sovrin Foundation
Founder, Internet Identity Workshop
Brigham Young University*

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