FREE SPEECH FOR PEOPLE .ORG

LACVAC
ELECTION PROTECTION

NVRTF
NATIONAL VOTING RIGHTS TASK FORCE

VALIDATE THE VOTE USA

Scrutineers

Our Cities, Our Counties, Our State
PDA-CA

AUDIT USA
Americans United for Democracy, Integrity and Transparency in Elections
Transparency is the Solution!
AUDIT USA
www.AUDITelectionsUSA.org

INDIVISIBLE★
MARIN

INDIVISIBLE
ALTA-PASADENA

INDIVISIBLE
Sacramento

INDIVISIBLE
SAN JOSE

INDIVISIBLE RIVERSIDE
including Moreno Valley, Jurupa Valley, Corona, Perris — CA
* From 2017 to 2021, we were "INDIVISIBLE 41", named after CA District 41. We're in CA-39 now :)

STAND STRONG LA
INDIVISIBLE

INDIVISIBLE SONOMA COUNTY

INDIVISIBLE
STANISLAUS

INDIVISIBLE
MENDOCINO

THE RESISTANCE
NORTHRIDGE ★ INDIVISIBLE

LONG BEACH ALLIANCE
FOR CLEAN ENERGY

INDIVISIBLE
CA ★ 33

INDIVISIBLE
MEDIA CITY ★ BURBANK

SOCAL
350
CLIMATE ACTION

ENVIRONMENTAL COMMITTEE
VALLEY WOMEN'S CLUB
Protecting Our Watershed

INDIVISIBLE
SOUTH BAY LA

LIVERMORE
INDIVISIBLE

Clean
Coalition

ROOTED IN RESISTANCE
rootsresist.org

Indivisible
Ross Valley

Cloverdale
indivisible

MOVI
MONEYOUTVOTERSIN

SEN

PUBLIC CITIZEN

ELECTRONIC FRONTIER FOUNDATION
EFF

Coalition for
Good Governance

April 19, 2022

The Honorable Steven M. Glazer, Chair
The Honorable Jim Nielsen, Vice Chair
The Honorable Robert M.Hertzberg
The Honorable Connie M. Leyva
The Honorable Josh Newman
Standing Committee on Elections and Constitutional Amendments
California State Senate
State Capitol Room 409/410
Sacramento, California 95814

Re: **SB 1480 STRONG OPPOSE**

Dear Chair Glazer and Members of the Committee,

Our organizations are dedicated to preserving and expanding voting rights and access, and to promoting secure, trustworthy election systems and policies. We have long supported responsible uses of technology to facilitate voting and increase access to the ballot box for all voters, especially voters with disabilities.

At present, voters with disabilities still experience significant barriers to casting their votes privately and securely,[1] and we should make efforts to resolve these challenges. In particular, we strongly support improving remote accessible vote by

[1] "Disability and Voting Accessibility in the 2020 Elections, Final Report on Survey Results." February 16, 2021. Rutgers University; U.S. Election Assistance Commission. *Available at:* https://smlr.rutgers.edu/sites/default/files/Documents/Centers/Program_Disability_Research/Disability_and_voting_accessibility_2020_election_Final_Report_survey_results.pdf

mail (RAVBM) in California, which allows voters with disabilities to electronically fill out and print ballots to be mailed in.

We also urge the Committee to explore expanding the use of Mobile Voting Vehicles, whereby election workers bring accessible voting devices to the residences and workplaces of voters with disabilities. These accessible devices allow disabled voters to privately and independently cast a secured, verifiable paper ballot with accessible technology. (Currently San Francisco and its neighboring counties have launched such an effort.[2])

But the *electronic* return of voted ballots, either by facsimile or electronic ballot return system, creates profound, dangerous, and currently unsolvable security vulnerabilities, and is unacceptably insecure. There is no technology currently available or expected in the foreseeable future that can adequately secure elections when ballots are faxed/electronically transmitted over the Internet.

At a time when election security and public confidence in our elections are under attack, increased electronic return of voted ballots, whether from a phone, tablet, or computer, is simply not safe or secure in any form. Furthermore, with the ongoing conflict in Ukraine, the threat of Russian cyber attacks on our election infrastructure has increased.[3] Election security is a matter of the highest U.S. national security, so we would be taking a very grave risk to our democracy any time the threat of foreign interference is escalated, as it is now.

We urge you to withdraw SB 1480, or for the Elections Committee to vote NO on SB 1480. We expand on our reasoning in the points below.

I. Returning voted ballots by facsimile is *Internet voting* which is inherently insecure.

[2] San Francisco, Oakland, San Jose and some of the twelve counties that surround it have invested a $1 million federal grant to provide Mobile Voting Vehicles to increase voting access to disabled and underserved voters. See: http://www.bayareauasi.org/sites/default/files/resources/approval_2022_january_meeting_master.pdf, page 57.

[3] 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/*

SB 1480 would significantly expand the fax return of voted ballots, which is unacceptably insecure. Fax technology has evolved tremendously since the old days of the very slow standalone fax machines and fax modems that transmitted over voice-grade telephony lines. *Virtually all fax transmission today is done over the Internet*. Fax voting is thus just another form of Internet voting, with all of the profound security weaknesses shared by all Internet voting systems (i.e. weak sender authentication, malware on the sender's device, routing attacks, denial of service attacks, server penetration attacks, etc.)

But fax voting is much worse than that. Fax transmission protocols actually predate the Internet. They were never designed with security in mind in the first place. Anyone who deals with junk faxes every day knows that the identity of the sender is often forged (which is trivial to do) and thus there is no limit to the number of forged ballots one might receive. Nothing prevents Russians or other malicious actors from faxing thousands of forged ballots that ostensibly come from disabled voters.

From a total security point of view fax ranks at the very bottom-of-the-barrel of communication systems, right along with email. Faxed ballots, like email ballots, are not – and cannot be – end-to-end encrypted (without tools, training, and IT security support at both ends that is beyond the capability of most voters and election officials). And they can be modified in transit by companies that relay them.

Note also that fax balloting would not be free to the voter. The voter would need up sign up for an online faxing service.

Internet voting of any kind is a national security threat, which California has wisely recognized this in the election code by making it illegal to connect any part of the voting systems to the Internet. SB1480 threatens to scrap that by *requiring* either the fax-handling system or the electronic ballot return system for disabled voters to be connected to the Internet for weeks of early and election day voting. **Rather than extend the use of fax voting in California, we would instead urge you to actually eliminate fax voting entirely for UOCAVA voters, to finally and permanently secure California elections from remote Internet-based interference.**

II. Electronic vote by mail is *Internet voting*, which is inherently insecure.

SB 1480 would permit the Secretary of State to certify a "remote accessible vote by mail system" that enables the voter to return a completed ballot electronically, and it would require county elections officials to permit a voter with a qualifying disability to use this system. Though SB 1480 notably does not use the term "Internet voting," or "online voting," a "remote accessible vote by mail system" that returns ballots electronically is unquestionably just a form of Internet voting.[4]

Among national security experts and computer scientists, there is no debate: online voting (any electronic transmission of a voted ballot) 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 specifically advised "we recommend paper ballot return as electronic ballot return technologies are high-risk even with [risk-management] controls in place."[5] 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."[6]

DHS's blunt warning against the use of online voting echoed bipartisan recommendations from the U.S. 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."[7]

[4] According to the US Election Assistance Commission report "A Survey of Internet Voting," (February 2011) internet voting is defined as: "Any form of ballot delivery where a voter's ballot selections are returned to a tabulation system via the Internet." *Available at: https://www.eac.gov/sites/default/_les/eac assets/1/28/SIV-FINAL.pdf*

[5] "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*

[6] Ibid.

[7] 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

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

III. As written, SB 1480 seems to permit Internet voting for *all* voters.

California code 3016.7(a) currently permits *all* voters to cast a ballot using a certified electronic vote by mail system. At present, that means that all voters can access a blank ballot electronically to mark it and mail it back.

Though this may not be the intention, if SB 1480 were to be enacted, and the Secretary of State certified an electronic vote by mail system that included the electronic ballot return technology, *all* California voters would be able to vote over the Internet. This would profoundly undermine any and all election security safeguards California has adopted. The damage this could do to California, and the nation's elections cannot be overstated - elections in California, the largest state in the nation, would be untrustworthy and unverifiable.

IV. Amendments to SB 1480 do not resolve the security concerns.

Since it was introduced, SB 1480 has been amended to no longer "direct" the Secretary of State to certify an electronic vote by mail system by April 1, 2023, but to "permit" the Secretary of State to certify a system, with no date specified. Though this amendment corrects a faulty proposal that disregards the Secretary's authority and discretion to determine if a system is worthy of California State certification, it does not resolve the security problems associated with electronic voted ballot return permitted in SB 1480.

Moreover, even as amended, SB 1480 ignores the fact that there are no standards for certification for electronic voted ballot return systems. This is not by accident. The National Institute of Standards and Technology (NIST) was directed by

[8] 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*

[9] Massachusetts Institute of Technology, 2020. "The Ballot is Busted Before the Blockchain: A Security Analysis of Voatz, the First Internet Voting Application Used in U.S. Federal Elections." https://internetpolicy.mit.edu/wp-content/uploads/2020/02/SecurityAnalysisOfVoatz_Public.pdf

Congress to develop standards for remote electronic ballot return over a decade ago. After many years of research NIST concluded it could not establish standards for secure electronic ballot return, because secure online ballot return is not feasible.[10] NIST's conclusion has been since reaffirmed by the Cybersecurity and Infrastructure Agency (CISA)[11] and NASEM.[12]

V. Electronic signature images cannot reliably authenticate voters.

SB 1480 would allow the Secretary of State to certify systems in which ballots can be remotely submitted and verified with an *electronic signature image* instead of a *wet ink signature on paper*. This would be a terrible practice since electronic signature images do not offer any real authentication at all. Successfully forging a wet ink signature is difficult, time consuming, and can only be done with skill and practice, and doing it successfully the first time on mail-in envelopes is essentially impossible. But an electronic signature image attached to an online ballot can be trivially forged by cutting and pasting, and anyone with an example of the signature can do it. An attacker with a collection of voter signatures can automate the forging process and impersonate many voters essentially undetectably. Use of signature images for authentication opens the door to scalable voter impersonation, and should not be permitted under any circumstances.

VI. Conclusion

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 to improve secure innovations, such as RAVBM or mobile accessible voting. However, internet voting, with or without blockchain, is not the answer. The 2020 election underscores the importance of being able to examine voted paper ballots, not just digital artifacts. A recent report published in the Journal of Cybersecurity warns, "While current election systems are far from perfect, Internet- and

[10] See: NIST Activities on UOCAVA Voting. Available at: https://www.nist.gov/itl/voting/uocava-voting

[11] See *supra* note 5.

[12] See *supra* note 8.

blockchain-based voting would greatly increase the risk of undetectable, nation-scale election failures.”[13]

We would welcome the opportunity to provide the Committee with further information on technical aspects of internet voting. We urge the California legislature in the strongest possible terms not to authorize the certification, adoption, testing, or development of any form of Internet voting to preserve the security voting in California, and voters’ confidence in the elections process.

Thank you for your consideration.

Sincerely,

Susan Greenhalgh
Senior Advisor for Election Security
Free Speech For People

Stephanie Chaplin
Lead
Secure Elections Network

Jim Soper
Chair
National Voting Rights Task Force

Cynthia Shallit
Enviro Committee
Indivisible Sacramento

Dr. David Jefferson
San Ramon, California
Election Integrity Foundation*
Lawrence Livermore Laboratories*
(retired)

Lecia Elzig
President
Indivisible Riverside

Emily Levy
Executive Director
Scrutineers.org

Kayla Owens
Enviro Director
Resistance Indivisible Northridge

Philip B. Stark
Professor, University of California, Berkeley*
Board of Advisors, U.S. Election Assistance Commission*
Board of Directors, Election Integrity Foundation*
Board of Advisors, Open Source Election Technology Institute*

[13] Sunoo Park, Michael Specter, Neha Narula, Ronald L Rivest, MIT, Going from bad to worse: from Internet voting to blockchain voting, Journal of Cybersecurity, Volume 7, Issue 1, 2021, https://doi.org/10.1093/cybsec/tyaa025

Michele Sutter
President & Co-Founder
MOVI, Money Out Voters In

Jennifer Tanner
Organizer
LA County Voters Action Coalition
Director
Validate the Vote USA.org

John Brakey
Director
Audit USA

Mike Thallier
President
PDA-CA

Susan Morgan
Leader
Indivisible Marin

Ruth Richardson,
Co-Leader
Rooted in Resistance (Indivisible)

Doug Bender
Enviro lead
Indivisible South Bay LA

Mary Perner
Leader
Livermore Indivisible

Vicky Groom
Leader
Cloverdale Indivisible

Yvonne Elkin
Leader
Indivisible Resistance San Diego

Larry Martin
Leader
Indivisible Sonoma County

Rebecca Elliot
Admin
Indivisible San Jose

Jack Eidt
Director
SoCal 350

Sue Sanders
Chair
Indivisible Ross Valley

Anita Ghazarian
Co-Chair
Indivisible Alta Pasadena

Duane Bundschadler
Leader
Indivisible CA-33

Chrisie Olson Day
Enviro Committee
Indivisible Mendocino

Marty Perimutter
Co-Leader
Indivisible Media City Burbank

Darlene Patrick
Leader
Indivisible Stanislaus

Janeen Pederso
Leader
Indivisible Stand Strong LA

Dave Shukla
Operations
Long Beach Alliance for Clean Energy

Ben Schwartz
Manager
Clean Coalition

Dorothy Reik
President,
Progressive Democrats of the Santa Monica Mountains

Nancy Macy
Lead Organizer
Valley Women's Club of San Lorenzo Valley

Aquene Freechild
Campaign Director, Democracy Is For People
Public Citizen

Hayley Tsukayama
Senior Legislative Activist
Electronic Frontier Foundation

Marilyn Marks
Executive Director
Coalition for Good Governance

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