

1 SAN FRANCISCO ELECTIONS COMMISSION

2 **RESOLUTION ON INTERNET VOTING**

3 (Adopted by the San Francisco Elections Commission (6-0) on April 19, 2017.)

4
5 **Resolution opposing internet and email voting in local, state, and federal elections.**

6
7 WHEREAS, The San Francisco Elections Commission (“Elections Commission”) on
8 August 20, 2008 adopted a “Policy on Favoring Paper Balloting over Other Forms,” stating in
9 part that—

10 (a) “[direct-recording electronic] (DRE) voting systems capture a vote and store it on a
11 memory card rather than mark a paper ballot”; and that

12 (b) “significant numbers of voters continue to have misgivings about votes not being
13 cast on a paper ballot, believing that it provides inferior security and inferior ability to
14 conduct a meaningful recount if one is necessary”; and adopting as policy that

15 (c) “the San Francisco Department of Elections shall operate in all its functions so as to
16 prefer the use of paper ballots (either marked by hand with the current system or
17 marked with the assistance of a machine designed for disabled access in future
18 systems) over the use of DRE voting,” consistent with any legal requirements;

19 WHEREAS, Internet voting systems, including returning marked ballots by email, do
20 not involve casting paper ballots, meaning there is no meaningful or independent way to
21 audit, recount or correct results in the case of electronic error or tampering;

22 WHEREAS, Internet voting is fraught with even more risk than DRE voting, because it
23 exposes local election jurisdictions to foreign governments, potential adversaries, and

1 malicious actors located anywhere in the world—enabling large-scale, sophisticated,
2 automated, undetectable, and uncorrectable vote tampering;

3 WHEREAS, The San Francisco Voting Systems Task Force, in its June 2011 report,
4 concluded in part that—

5 (a) “anyone anywhere with Internet access has the ability to target remote digital voting
6 systems in order to carry out the same type of Internet-based attacks that have
7 succeeded against several organizations with security expertise that far exceeds that
8 of any voting system vendor or election jurisdiction—including Google, Adobe, RSA
9 Security, and dozens of other large corporations”; and that

10 (b) “the use of remote digital voting—especially the digital return of voted electronic
11 ballots with no audited paper ballots—is far too insecure in public elections application
12 for the foreseeable future”; and that

13 (c) “the official 'ballot of record' should be a paper artifact”;

14 WHEREAS, The Elections Commission on November 18, 2015 adopted a resolution
15 “that it be the position of the Elections Commission that open voting systems using paper
16 ballots have the potential to provide the greatest degree of accessibility, accuracy,
17 transparency, security, auditability, affordability, and flexibility in elections, and so would best
18 serve the voters of San Francisco”;

19 WHEREAS, Reports of the hacking of major corporate and government computer
20 networks are a regular occurrence in the news—affecting the networks of organizations
21 including JP Morgan, Bank of America, Wells Fargo, Charles Schwab, Visa, Mastercard,
22 Yahoo, Symantec, the CIA, the FBI, the Pentagon, INTERPOL, and NATO—not to mention
23 incidents that go unreported due to being undetected or not disclosed;

1 WHEREAS, Voting differs fundamentally from banking and other types of transactions
2 because in banking customers can check transactions and have mistakes corrected; whereas
3 with voting, a ballot cannot be linked back to the voter once it has been cast;

4 WHEREAS, Last year, the Democratic National Committee's email system and the
5 voter registration systems of Illinois and Arizona were hacked, leading the FBI to publish a
6 security alert and the Department of Homeland Security to declare our election infrastructure
7 to be a “critical infrastructure subsector”;

8 WHEREAS, Fully protecting an election management system or voting system from
9 insider or outsider attacks by hackers, programmers, or election administrators is not possible
10 in the foreseeable future;

11 WHEREAS, Protecting the average voter's computer, be it a desktop or smartphone,
12 from an endless and ever-evolving array of malware, fake apps and malicious websites is not
13 possible in the foreseeable future;

14 WHEREAS, In just thirty-six hours a team of University of Michigan computer scientists
15 penetrated an internet voting system about to be used by Washington DC; and in doing so
16 obtained control of every part of the system—including votes, vote totals, passwords,
17 tabulator, encryption codes, databases, voter records, and cameras—causing officials to
18 cancel the project;

19 WHEREAS, No national standards exist for internet voting systems, and the National
20 Institute of Standards and Technology (NIST) has stated that “Internet voting systems cannot
21 currently be audited with a comparable level of confidence in the audit results as those for
22 polling place systems. Malware on voters' personal computers poses a serious threat that
23 could compromise the secrecy or integrity of voters' ballots. And, the United States currently

1 lacks a public infrastructure for secure electronic voter authentication”;

2 WHEREAS, Sections 19205 and 19295 of the California Elections Code forbid
3 connecting any part of a voting or ballot marking system to the Internet, or to a wireless,
4 phone, or other external network;

5 WHEREAS, Democracy advocates, joined in the past by Secretary of State Debra
6 Bowen, defeated at least three previous attempts in the California legislature to introduce
7 some form of internet voting to California's elections, including SB 908 (2011-12); AB 19
8 (2013-2014); and AB 887 (2015-16);

9 WHEREAS, AB 1403 (2017–18), “Military and overseas voters: return of ballot by
10 email,” represents yet another attempt to introduce internet voting into California's elections;

11 WHEREAS, In Canada, where internet voting is being tried in some municipal elections
12 in Ontario for example, British Columbia's Independent Panel on Internet Voting conducted a
13 review and issued its "Recommendations Report to the Legislative Assembly of British
14 Columbia – February 2014," recommending not to implement universal internet voting and
15 concluding in part that—

16 (a) "research suggests that Internet voting does not generally cause non-voters to vote.
17 Instead, Internet voting is mostly used as a tool of convenience for individuals who
18 have already decided to vote"; and that

19 (b) "Internet voting is most popular among middle-age voters and least popular among
20 youth and therefore reflects traditional voter turnout demographics. These findings run
21 contrary to the widely expressed belief that Internet voting will lead to increased
22 participation by youth";

23 WHEREAS, The seeming convenience of internet voting is overshadowed by the fact

1 that votes cast by computer and transmitted over the internet are especially vulnerable to
2 being changed or eavesdropped upon, subverting both voter intent and ballot secrecy and so
3 the integrity of the ballot itself;

4 WHEREAS, The integrity of our country's elections depend on the integrity of ballots,
5 election technology and processes used not just locally but across the country;

6 WHEREAS, In July 2015, a team of election officials, computer security experts, and
7 experts in disability, usability, auditing, testing, and legal issues published a thorough,
8 136-page report entitled, "The Future of Voting: End-to-End Verifiable Internet Voting
9 (E2E-VIV) – Specification and Feasibility Study," which in part—

10 (a) defined "end-to-end verifiable" as, "First, every voter can check that his or her ballot
11 is cast and recorded as he or she intended. Second, anyone can check that the system
12 has accurately tallied all of the recorded ballots";

13 (b) contained an extensive and rigorous set of requirements that any internet voting
14 system should satisfy; and

15 (c) concluded by saying, "It is currently unclear whether it is possible to construct an
16 E2E-VIV system that fulfills the set of requirements contained in this report"; now,
17 therefore be it

18 RESOLVED, That it be the policy of the Elections Commission to oppose allowing
19 votes in United States local, state, and federal elections to be cast over the internet, including
20 by email.