SAN FRANCISCO ELECTIONS COMMISSION

RESOLUTION ON INTERNET VOTING (PROPOSED / DRAFT)

Date: April 14, 2017

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

WHEREAS, The San Francisco Elections Commission ("Elections Commission") on August 20, 2008 adopted a "Policy on Favoring Paper Balloting over Other Forms," stating in part that—

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

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

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

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

WHEREAS, Internet voting is fraught with even more risk than DRE voting, because it exposes local election jurisdictions to foreign governments, potential adversaries, and malicious actors located anywhere in the world—enabling large-scale, sophisticated,

automated, undetectable, and uncorrectable vote tampering;

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

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

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

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

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

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

WHEREAS, Voting differs fundamentally from banking and other types of transactions

because in banking customers can check transactions and have mistakes corrected; whereas with voting, a ballot cannot be linked back to the voter once it has been cast;

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

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

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

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

WHEREAS, No national standards exist for internet voting systems, and the National Institute of Standards and Technology (NIST) has stated 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”;

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

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

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

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

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

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

WHEREAS, The seeming convenience of internet voting is overshadowed by the fact that votes cast by computer and transmitted over the internet are especially vulnerable to

being changed or eavesdropped upon, subverting both voter intent and ballot secrecy and so the integrity of the ballot itself;

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

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

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

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

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

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

FINALLY RESOLVED, That the Elections Commission reserve the right to revisit this issue if and when enough theoretical and practical advances have been made to warrant a reassessment of whether internet voting can be done securely, verifiably, usably, and transparently.