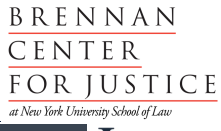

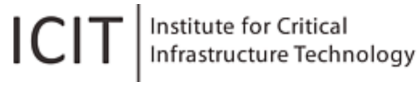

August 13, 2018

Hon. Roy Blunt (*via email*)
U.S. Senate
260 Russell Senate Office Building
Washington, DC 20510

Hon. Amy Klobuchar *(via email)*
U.S. Senate
302 Hart Senate Office Building
Washington, DC 20510

RE: Secure Elections Act

Dear Senator Blunt and Senator Klobuchar:

The organizations who are signatories to this letter have been working over the last year and a half to urge Congress to enact legislation that protects American democracy by advancing secure, verifiable, and auditable voting systems. We are gratified by the bipartisan Senate sponsorship that the Secure Elections Act has received, which reflect that election cybersecurity is a matter of national security, not a partisan issue.

We have learned that the co-sponsors of the SEA are poised to introduce a revised version of the bill. We have not seen the language in the new version but feel compelled to write to you to advocate again for strong language that will shore up the machinery of democracy rather than leave it vulnerable to attack.

We recognize that each state faces unique challenges and constraints, and that an overly prescriptive approach will not be successful. However, in our collective view—which represents a broad swath of subject-matter experts in computer science, cybersecurity, and election administration, as well as people from every point on the political spectrum—the SEA must reflect the following principles in order to effectively secure the voting process:

There must be a requirement (or strong incentive) for electronic voting systems to incorporate **a paper ballot (marked by hand or device) that is visible to the voter and retained for**

audits or recounts. With equal importance, there must be a requirement (or strong incentive) for federal contests to be subject to **manual post-election audits, in which people inspect a random sample of the paper ballots (by hand *and not* by device) and the number of ballots inspected is sufficient to establish high statistical confidence in the reported outcome**.

The reasons for voter-verified paper ballots and manual post-election audits have been discussed at length, but it bears repeating that this combination of safeguards is *the only practical defense* that can reliably detect and correct cyberattacks against voting machines. This is not only our assessment; NIST researchers reached the same conclusion[1]. Voter-verified paper ballots provide evidence of voters' intent that cannot be changed in a cyberattack, and manual post-election audits use that evidence to detect any faults in the computerized counting process and, if necessary, recover from those events. Although other procedures and safeguards are important, only voter-verified paper ballots and manual audits provide robust assurance that elections outcomes cannot be manipulated in a cyberattack.

Both voter-verified paper ballots and manual post-election audits are essential components of this defense, and neither offers sufficient protection without the other. An electronic voting system that incorporates both provides a cost-effective, failsafe disaster-recovery plan that will bolster confidence in our democracy.

We understand the challenges that passage of the SEA presents, and the months of hard work that the sponsors have invested so far. Nevertheless, the effectiveness of the bill, and thus our support, depends upon strong language that prevents unverifiable systems or superficial audits from perpetuating the vulnerabilities of American election systems.

We would be happy to discuss our concerns with you at any time. Thank you for your consideration.

Respectfully,

Americans for Tax Reform

Brennan Center for Justice

Common Cause

Freedom Works

Institute for Critical Infrastructure Technology

The London Center

---

[1] https://www.eac.gov/assets/1/28/AuditabilityReport_final_January_2011.pdf

National Election Defense Coalition

Project on Government Oversight

Verified Voting

cc: Senate co-sponsors of the Secure Elections Act *(via email)*