



June 22, 2017

Chairman Richard Burr

Vice Chairman Mark Warner

The Honorable Roy Blunt

The Honorable Susan Collins

The Honorable John Cornyn

The Honorable Tom Cotton

The Honorable Dianne Feinstein

The Honorable Kamala Harris

The Honorable Martin Heinrich

The Honorable Angus King

The Honorable James Lankford

The Honorable Joe Manchin

The Honorable Jim Risch

The Honorable Marco Rubio

The Honorable Ron Wyden

Dear Senators,

Verified Voting vigorously applauds the Senate Select Committee on Intelligence for its leadership and commitment to securing our elections. With clear evidence that foreign attackers sought to attack our 2016 elections through various means, our intelligence agencies warn that hostile attackers will be back to attack future elections. Congress and the most vulnerable states should act with urgency to fund and implement protective reforms that will make our election systems resilient against cyber attack: funding the adoption of paper ballots and accessible ballot marking systems, and implementing robust, manual post-election audits of the votes.

The June 21 hearing is an important first step toward those reforms, providing valuable information through witness testimony and questions of the Senators. We wish to expand on several key points that were raised in the hearing to ensure a clear understanding of the challenges we face in securing our elections.

It is crucial to understand that further reforms are urgently needed to bolster the mitigations currently in place so that it is possible to *detect* and *correct* a cyber attack on the vote count.

Some testimony asserted that pre-election testing and post-election audits currently in place would catch errors in vote tallies caused by a malicious attacker or software failure. Unfortunately, pre-election testing, though helpful for ensuring the completeness of ballot programming, can be defeated by malicious software designed to detect when the system is in test mode. This is what happened with Volkswagen diesels cars: the software caused the cars' emissions systems to behave correctly during testing, but then allowed them to pollute under non-testing conditions.

Likewise, while post-election audits currently in place in some states may serve to detect errors in the vote count—and indeed in a number of past elections have detected outcome-changing errors—*such audits cannot be relied upon nationally*. A post-election audit requires examination of some number of paper ballots marked by voters, to serve as a check on the software vote count. Because voters in five states are consigned to paperless machines, and nine other states contain jurisdictions that do not have paper ballots, it is impossible to conduct a legitimate post-election audit to detect software errors in 14 states.

Moreover, while roughly 70% of the nation has paper ballots,<sup>1</sup> little more than half the country conducts post-election audits<sup>2</sup> and, with few exceptions, these audits are not strong enough to always reliably detect vote count errors caused by cyber attacks or software problems. This is why we need paper ballots and robust post-election audits: to have sufficient evidence to detect and correct errors in all jurisdictions, not just in some jurisdictions.

Although most voting machines are not directly connected to the Internet, they nonetheless may be exposed to hacking attacks through other connections, as Dr. Alex Halderman explained in his testimony.<sup>3</sup> Furthermore, 32 states allow the online casting of ballots for military and overseas voters;<sup>4</sup> these ballots are directly exposed to Internet attacks. Because these ballots are cast electronically, their accuracy cannot be verified or accurately audited.

At the hearing, Senators pressed the important point that our current system does not ensure that State election directors will disclose breaches to the public or other entities. In some localities, election systems are managed by outside vendors, some of which may not have the resources to implement strong security. In these cases the vendors would be responsible to detect and report vulnerabilities or intrusions. But vendors may feel a financial and reputational disincentive to disclose vulnerabilities or breaches of their systems. Without reforms to require such disclosure, we cannot reasonably expect to learn of all breaches and vulnerabilities. This exacerbates the difficulty of addressing security challenges.

---

<sup>1</sup> <https://www.verifiedvoting.org/verifier/>

<sup>2</sup> <https://www.verifiedvoting.org/resources/post-election-audits/>

<sup>3</sup> Expert Testimony by J. Alex Halderman, Professor of Computer Science, University of Michigan before the Senate Select Committee on Intelligence June 21, 2017

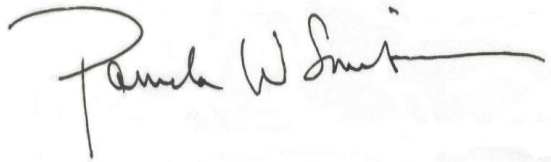
<https://www.intelligence.senate.gov/sites/default/files/documents/os-ahalderman-062117.pdf>

<sup>4</sup> "Secret Ballot at Risk, Recommendations for Protecting our Democracy," Verified Voting Foundation, Common Cause, Electronic Privacy Information Center, <http://secretballotatrisk.org/>

Paper ballots and post-election ballot audits provide resilience to cyber attacks on our voting process, because the paper ballot is physical, tangible evidence of voter intent that will remain untouched by a cyber attack. In the hearing we were told that one of our adversaries' aims is to sow distrust in our elections so as to undermine U.S. democratic principles. Paper ballots and audits provide transparency and instill voter confidence in the process. By combining paper ballots with routine, mandatory post-election manual audits, we directly and effectively undercut our adversaries' ability to shed doubt on the election outcome. Voters will have evidence to support the computer tallies, improving both transparency and voter confidence.

We thank you for focusing on this critical issue and for your commitment to address it. We hope to work with you to move the entire nation to resilient, auditable, transparent and accessible voting systems and stand ready to assist any way we can.

Very truly yours,

A handwritten signature in black ink that reads "Pamela W. Smith". The signature is written in a cursive style with a long horizontal flourish at the end.

Pamela Smith  
President