America's voting systems need security upgrades: It's time to beef up cybersecurity

By R. James Woolsey and Tony Shaffer | May 12, 2017

There's no evidence that hacking had any impact whatsoever on the results of the 2016 election. But—in an age of rapidly rising cybersecurity threats and quickly aging voting infrastructure—there's no guarantee that elections in 2018, 2020, and beyond will be safe. While alleged Russian hacking has received huge attention this year, the cyber-threat to American electoral democracy could come in the future from Russia, China, North Korea, ISIS, or any of a number of players with cyber capacities.

This is a serious matter of national security. Policymakers should treat it as such. It's no secret that America's voting systems need security upgrades. According to a recent study, 43 states use electronic voting and tabulation systems that are at least a decade old — dangerously near to the estimated lifespan for such systems. A survey of 274 election officials in 28 states found that most administrators need upgrades. Antiquated systems are inherently more vulnerable to hacking. There are now 52 different kinds of voting machines in use around the country, including Direct Recorded Electronic (DRE) machines and optical scanning machines. Agents can tamper with these systems by gaining brief physical access, by inserting a memory card, or by remotely hacking computers on which systems are programmed.

Federal policymakers helped sow the seeds of this insecurity nearly two decades ago, when, after the "hanging chad" fiasco of the 2000 election, the government spent billions on the purchase of voting machines without paper ballots — or even paper trails — and few, if any, cybersecurity safeguards.

We need hardened cybersecurity for America's voting systems. Local control of elections is essential and Congress can't solve the problem alone. Still, federal agencies should seek to undo the damage of earlier policy decisions by setting high-quality national standards for cybersecurity as a condition of new federal funding for voting systems. Ultimately, we believe the solution to election insecurity lies in President Reagan's famous old adage: "trust but verify"—say by paper trails permitting valid recounts. We should trust that America's votes are being counted correctly, but we should be able to verify that this is, in fact, the case. Verification requires the presence of at least a paper trail: voter-marked paper ballots that can be used to check the results, if necessary, of the electronic tally.

This used to be the norm in American voting systems, and it should be once again. Paper ballots are both cost-effective and secure. On the morning of Election Day, November 8th, President Trump went on Fox News to explain his views on the issue: "There's something really nice about the old paper ballot system," he said. "You don't worry about hacking." The President is right. We need to return to safe and simple elections with paper ballots providing the check against the electronic tally.

R. James Woolsey was Director of Central Intelligence 1993-1995. Lt. Col. Tony Shaffer is Vice President for Operations of the London Center for Policy Research, a New York City-based national security think tank.