The Washington Post

We need to hack-proof our elections. An old technology can help.

By Michael Chertoff and Grover Norquist

February 15, 2018

Michael Chertoff was secretary of homeland security from 2005 to 2009. Grover Norquist is president of Americans for Tax Reform.

The nation's top intelligence officers warned Congress this week that Russia is continuing its efforts to target the 2018 elections.

This should come as no surprise: A few months ago, the Department of Homeland Security notified 21 states that hackers had targeted their election systems in 2016. Yet Congress still has not passed legislation to meaningfully address election cybersecurity.

Time is running out. Lawmakers need to act immediately if we are to protect the 2018 and 2020 elections.

There's no evidence that vote totals were hacked in 2016. But it's obvious that hackers have been testing the waters. Our attention has focused on Russia, but future threats could also come from North Korea, China, hacking groups such as Anonymous or any other adversary — foreign or domestic.

It should also be no surprise that hackers have U.S. voting systems in their sights. They're a relatively easy target. Researchers have studied a range of electronic voting infrastructure — including touch screens, optical scanner systems and registration databases — and found serious vulnerabilities that could allow even moderately sophisticated attackers to pose threats to voting integrity. This year, about 40 states are set to use electronic voting or tabulation systems that are more than a decade old — many of which run on software that's too old to be serviced with vendor security patches. A survey of nearly 300 election officials in 28 states found that a clear majority report needing new voting systems.

We believe there is a framework to secure our elections that can win bipartisan support, minimize costs to taxpayers and respect the constitutional balance between state and federal authorities in managing elections. In September, Mark Meadows (R-N.C.), who chairs the conservative House Freedom Caucus, introduced legislation that would help solve the problem with an elegantly simple fix: paper ballots. Meadows's Paper Act would authorize cost-sharing with states for the replacement of insecure electronic systems with those that produce a voter-verified physical record. The bill also lays the groundwork for states to regularly implement risk-limiting audits — procedures that check a small random sample of paper records to quickly and affordably provide high assurance that an election outcome was correct.

President Trump has already endorsed this framework, declaring: "There's something really nice about the old paper ballot system. . . . You don't worry about hacking." And in the Senate, a bipartisan group of six lawmakers recently introduced the Secure Elections Act, which presents a sweeping set of security fixes including federal grants to install systems that use voter-verified paper ballots. The best estimates show that we can replace all paperless voting machines in the United States for about the cost of a single F-22 fighter jet — and in fact, the Senate bill would not add to the deficit because it offsets any new spending.

Both the House and Senate bills rightly defend the constitutional principle that states and localities should have primary responsibility over election administration. But they also acknowledge that federal authorities have a role in elections to "provide for the common defense." Rather than creating new federal mandates, the reform proposals look to identify the best thinking on election security and create guidelines for the use of federal funds.

It's not practical to expect local election administrators in rural Missouri or small-town Maine to go toe-to-toe with the premier government-backed cyber-mercenaries of China or North Korea. Just as federal agencies prudently provide support for state law enforcement in dealing with terrorism, federal officials should give guidance and support in dealing with the election cybersecurity threat.

If there's one takeaway from the past year's endless parade of high-profile cyberattacks, it's that everyone — from consumers to small businesses to global firms — is at risk. With recent revelations of sophisticated cyberattacks against voting systems in the United States and abroad, it's clear that anyone running for public office is at risk, too. Members of Congress should recognize that election cybersecurity reforms are in their own personal interest — and in the interest of the United States' national security.