TRIB LIVE

Safeguarding the election: The wrong remedy

September 18, 2016

The security of U.S. elections are sacrosanct. That's precisely why talk of the federal government stepping in to “protect” election systems deserves no vote of public confidence.

Department of Homeland Security Secretary Jeh Johnson has said he's considering designating election systems as “critical infrastructure” after reports of hacked voter registration information, possibly by Russians, in Arizona and Illinois. But the rationale for this intrusion is meritless.

The USA Patriot Act and Homeland Security Act define “critical infrastructure” as “systems and assets … so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.”

A hacked election, in one state or more, would be bad enough. But it wouldn't prevent the U.S. from functioning, reminds Brad Smith, a Capital University law professor.

By shoving its “nose under the tent,” the federal government would introduce far more problems than it would solve. Security against voting machine hacking is reinforced by the fact that U.S. election systems are decentralized. They're not in a network. Rather, there are about 9,000 different election jurisdictions, says Ilya Shapiro of the Cato Institute.

In era of increasing cyber threats, opening a door to federal intrusion in state election systems would be an especially perilous move.