Protecting American Votes and Elections Act of 2019 (S. ___)

The 2016 elections highlighted long-standing security flaws in America's election infrastructure. This bill secures Federal elections from foreign meddling by mandating paper ballots and routine, post-election "risk-limiting" audits. It gives DHS the power to set mandatory security standards for voting machines, voter registration databases, and election results websites used in Federal elections. The bill authorizes a $500 million one-time grant program to pay for states to buy new ballot scanning machines, which are needed to count paper ballots. Under this bill, the federal government will also reimburse states for the cost of designing and printing paper ballots and for conducting risk-limiting audits. The bill also protects the confidentiality of votes cast by people with disabilities, by providing states $250 million to buy new ballot marking machines.

Why do we need paper ballots?

DHS Secretary Nielsen, echoing the advice of experts, has called on "state and local election officials to make certain that by the 2020 presidential election, every American votes on a verifiable and auditable ballot." In 2018, five states relied exclusively on insecure, paperless voting machines and 9 more states used paperless machines in at least some jurisdictions. Votes cast with paperless voting machines cannot be subjected to a manual recount, and so there is no way to determine the real election results if they are hacked. H.R. 1 also mandates paper ballots.

What are risk-limiting audits and why do we need them?

In order to detect hacks, this bill requires election bodies to conduct audits of all federal elections, regardless of how close the election, by employing statistically rigorous "risk-limiting audits." These audits deliver nearly the same level of confidence in election results as a full manual recount, at a fraction of the cost. Colorado, Rhode Island, and Virginia currently mandate risk-limiting audits. In contrast, 16 states do not mandate any routine, post-election audits, while many others only require recounts in a few precincts. That is insufficient to detect election hacks.

Why do we need mandatory election cybersecurity standards?

There are currently no mandatory standards for election cybersecurity, which has resulted in some states operating election infrastructure that is needlessly vulnerable to hacking. The Election Assistance Commission (EAC) sets voluntary standards for voting machines, but states can and do ignore these standards. There are no standards at all for voter registration websites or other parts of our election infrastructure. Not only do the existing voluntary standards not work, but it's clear the EAC is the wrong agency to be in charge of election security. The EAC was established by Congress to distribute grant money. Commissioners are not chosen for their cybersecurity knowledge, and the Commission lacks in-house cybersecurity expertise. The Cybersecurity and Infrastructure Security Agency in DHS is far better suited to that task.

The security of Federal elections cannot be left to the states

State and local governments will never have the resources to defend against cyber attacks by foreign intelligence services. This is a national security issue, which requires federal action. The election clause in the Constitution clearly gives Congress the power to set standards for Federal elections. Consistent with the Constitution, none of the mandates apply to state or local elections.