Background: Safeguarding Elections August 2017

There is no evidence that hacking had any impact on the results of the 2016 election. But—with rising cybersecurity threats and aging voting technologies—elections in 2018 are deeply insecure. Future risks to elections could come from North Korea, ISIS, Anonymous, or other adversaries. These recommendations center on enabling use of paper ballots and risk-limiting audits—empowering states to address attacks, without reliance on the federal government:

How America's adversaries could target *voting technologies*

- Remote hack of state or county election night reporting, misrepresenting vote totals from precincts and casting doubt on accuracy of voting machines.
- Infect removable memory cards used in each voting machines with a vote-altering virus (potentially by hacking election vendors that typically program machines).
- Gain physical access to voting machines, causing them to "flip" voter choices on screens and creating doubt as to whether voters' choices were accurately recorded.

Policy Solutions: Secure voting technologies

1. **Restore Paper Records:** Ensure each vote in a federal election is accompanied by a paper record that the voter sees before casting a ballot. The cost of replacing *all* paperless machines (which exist in 14 states) would be between $130 million and $400 million. This cost could be shared with states through time-limited grant programs.
2. **Risk-Limiting Audits:** Conduct post-election audits of machines, using paper record to prove with high level of statistical confidence that machine totals are accurate. Implementing audits across the country would cost less than $20 million annually.

How adversaries could attack *voter registration systems*:

- Hack into statewide voter registration database and delete names or change addresses, so voters' names are not on rolls when they show up to polls or request absentee ballot.
- Hack into local voter registration database and add names and addresses, request absentee ballot, and mark voter as having presented adequate ID.
- Delete whole databases or use "denial of service" attacks to make systems crash just before Election Day, hampering ability of poll workers to sign voters in.

Policy Solutions: Securing voter registration systems

1. **Cybersecurity Support:** Provide time-limited grants to states to conduct risk analysis and replace insecure IT infrastructure where needed. 42 states are using statewide registration databases that were created at least a decade ago. Many databases run on discontinued software like Windows 2000 that is more vulnerable because it is no longer vendor-supported.
2. **Strengthen Failsafes:** Ensure that states and localities have sufficient training and staff to implement election day failsafes. Most jurisdictions have contingency plans that should allow them to recover from attacks, including by relying on provisional ballots. But many lack staff and training to follow through when an emergency arises.