LDF
LAWYERS DEMOCRACY FUND

Analysis of the Secure Elections Act

- The Secure Elections Act (S. 2261) was introduced on December 21, 2017. It is sponsored by Senator James Lankford of Oklahoma and co-sponsored by a bipartisan group of senators.

- Its purpose is to protect the administration of federal elections against cybersecurity threats. While better than some recent legislation that has been introduced to improve security in elections, there are some significant problems with this legislation in its current form.

- First, it imposes onerous reporting requirements on state and local election officials.
    - Within three calendar days of discovering a possible cybersecurity event, election officials must thoroughly analyze the event, develop a plan to "respond to and recover from" the event, and report these items to the Department of Homeland Security ("DHS") Secretary.
    - Election officials also have a continuing duty to report any updated information.
    - Similarly, "election service providers," defined broadly to include any person or entity "providing, supporting, or maintaining an election system" must report any possible cybersecurity events to local election officials and assist in their reporting obligations. This would include voting systems vendors, voter registration vendors, electronic poll book vendors, information technology support vendors, and many other private industry vendors.
    - "Election systems" is defined broadly as "any information system . . . used for the management, support, or administration of a Federal election." This would include voting systems in polling places, tabulators and election management systems in election board offices, election night reporting systems that publish results, voter registration systems at the state and local level, and even the election agency email system. These systems are often interconnected with state and local information technology systems overseen by separate, non-election officials.
    - Large jurisdictions may have the manpower and resources to compile such a comprehensive report within three days, but many small jurisdictions would struggle to prepare it so quickly.
    - Republicans are generally hesitant to impose such requirements on states and localities.
    - It is unclear what would happen if a state or local official refuses to report or adequately report, but the Act likely establishes a new independent federal requirement that would be enforced by the Department of Justice through litigation and consent decree.

- Second, it gives a tremendous amount of discretion to the Department of Homeland Security to establish ostensibly voluntary guidelines that will become mandatory in effect.
    - The nine-member advisory panel is controlled by the DHS Secretary. Five members are appointed by the DHS Secretary, and one each of the remaining four is selected by a different organization.
    - The advisory panel will be dominated by cybersecurity experts, not election experts. All five of the DHS appointees must be cybersecurity experts. The remaining four must be either cybersecurity, election law, or election administration experts.
    - The advisory panel has broad discretion to establish "standards for procuring, maintaining, testing, auditing, operating, and updating election systems" that must be met by states before receiving grant funds under the Act. Once the advisory panel has determined its standards, the DHS Secretary can change any guidelines developed by the advisory panel before they are submitted to Congress.

- This adds another advisory panel bureaucracy, complete with staff, when the Election Assistance Commission ("EAC") already has established advisory panels of experts working in this area.
- Because the standards will be required for states to receive funding, vendors will meet the standards in their election administration products and services, making the voluntary standards mandatory in practice. Currently, vendors meet EAC guidelines, which were developed by election officials and subject matter experts in security and accessibility in consultation with the National Institute of Standards and Technology and other organizations. The EAC currently tests all voting systems to privacy and security standards established by federal law and advisory boards and approved by the bipartisan EAC.

- Third, it opens the door to control of election administration by one political party or interest group.
  - Political appointees at DHS will control the advisory panel and standards process, enabling control by one political party. The existing agency for guidelines and grants, the EAC, has bipartisan structure and control of the process.
  - The advisory panel is designed to be controlled by cybersecurity experts, to the exclusion of election experts. The technology and security community has, to date, shown very little interest in the concerns and requirements of the election community and little desire to learn the underlying election administration issues that impact any security questions.