Talking Points on S. 2593 - "Secure Elections Act"
Amendment in the Nature of a Substitute Released August 17, 2018

Prepared on August 20, 2018

- This amended text is slightly better than the original Secure Elections Act, proposed in December 2017 (S. 2261). Senator Roy Blunt should be applauded for removing some of the most dangerous parts of the original proposal, such as the Department of Homeland Security ("DHS") Secretary's control of the new advisory panel and onerous reporting requirements for state and local election officials.
- Nevertheless, there are still concerns with the amended text.
- The amendment is still the most significant federal intrusion into the state administration of elections in history, requiring mandatory audits in every locality, reporting of cyber incidents to the federal government, the imposition of new election guidelines for election systems, and states to transition to paper balloting for future federal funds. All of these new federal mandates come with no additional monies to states and localities.
- Mandatory federal audits by local election officials implemented for the first time in a presidential election year will place significant burdens on local election officials and, in the current language, no federal candidate may be certified or sworn in until these audits are complete. This is opening election administration to a new round of voting wars litigation and messaging that will negatively impact voter confidence.
- Hearings have not been held on this amended text, and members should take more time to consider all its provisions.

Good Provisions in the Amended Version of the Act

- The federal-to-state information sharing provisions of Section 3 of the Act could provide valuable information about cybersecurity threats to state election officials. This type of communication was non-existent in 2016, and state election officials have struggled to receive any real-time classified information from the DHS or the federal government. There is no excuse for the continued delay of security clearances being provided to state election officials and the Election Assistance Commission ("EAC").
- Development of the new "voluntary election cybersecurity guidelines" and the new "voluntary election audit guidelines" under the bipartisan EAC, instead of under a new board controlled by the DHS Secretary and cybersecurity experts, who generally lack election experience or knowledge.

Specific Concerns with Amended Text

- The Act applies to any "election system," which is quite broadly defined.
    - It includes 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, electronic pollbooks, 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, which makes the application of this Act extremely broad.
    - The DHS Secretary, in consultation with the Election Assistance Commission, may identify additional "information systems" as election systems.
- While the amended Act has removed the onerous three calendar-day deadline for states or localities to provide a full report on any potential cybersecurity incident to the DHS Secretary, the new language requires a report "in the most expedient time possible and without unreasonable delay."
    - The removal of the three-day deadline is an improvement, but the new language is vague enough that DHS could create a similar deadline through regulations or procedures, as the DHS Secretary is given authority to establish a notification process.
    - Like the original Act, the amended Act still requires the report to contain a thorough analysis of the cybersecurity event and a plan to "respond to and recover from" the event. Election officials also have a continuing duty to report any updated information
    - Large jurisdictions may have the resources to compile such a comprehensive report during a busy election season and while actually addressing the threat itself, but many small jurisdictions would struggle to prepare it "without unreasonable delay."
    - The burden of identifying and reporting these vague incidents rests on election offices and local government information technology support offices and any agency supporting election offices. Members should be 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, as the Act specifically states that no cause of action is created by it. Whatever procedures are followed to attempt to enforce the Act would again take time and resources away from election officials performing their duty of administering elections.[1]
- The amended Act amends the Help America Vote Act of 2002 ("HAVA") to further constrain the states by conditioning receipt of any HAVA grants on a state establishing a "response and communication plan with respect to election cybersecurity incidents."
- Like previous "voluntary" federal standards for election-related systems and processes, the new voluntary election cybersecurity guidelines and the new voluntary election audit guidelines will become mandatory in effect as vendors conform standards to them and advocacy organizations sue states and localities that do not meet the "voluntary" standards.
- The "voluntary" election audit guidelines will require states to have a paper-based ballot system and conduct a random audit prior to a winning candidate being sworn in to office to establish "high statistical confidence" in the election result.
    - While these may be good practices, many states do not have the equipment or systems to accomplish these two tasks.
    - Conversion to paper-based ballot systems and audits are very expensive, and this is an unfunded mandate.

[1] Many state election officials and many of the over 6,000 local election officials across the country have duties in addition to administering elections.

    - States should be allowed to establish the election systems and procedures that will best protect their citizens' right to vote, as they best know the local circumstances and what is feasible in the state.
    - The Act repeatedly uses "high statistical confidence," which is in essence requiring a risk-limiting audit.
        - Risk-limiting audits require a massive dedication of time and resources in close elections, as a large number of ballots would need to be reviewed to develop "high statistical confidence" that the election outcome is correct.
        - Review of a smaller number of ballots is required in elections won by a large margin, but an audit is still a large expense and the outcome of the election is very unlikely to change.
        - Even counties with new digital scan voting equipment find risk-limiting audits to be burdensome and difficult to complete. Localities with older equipment will find it very difficult to impossible to meet these new requirements. There are few jurisdictions that currently conduct risk-limiting audits.
    - In the amendment, there is a requirement that no federal candidate race can be certified unless the audit is complete. There will be many jurisdictions unable to comply or timely comply, so there will be winning candidates for federal office who will not be allowed to be sworn in.
- In addition to the provisions of the "voluntary" guidelines, the Act would amend HAVA to require states to conduct a post-election audit.
    - Again, this is a new requirement for the states, not matched with any funding for the states to accomplish this expensive requirement.
    - States must implement a post-election audit by the November 2020 elections (though a waiver until November 2022 is available), which would require a massive, immediate appropriation of funds for new equipment in some states (in addition to time and expense training staff and volunteers on new equipment and all the election administration upheaval that comes with new equipment).
    - The audits will be implemented in a presidential election year and there are no training or educational provisions in the amendment.
    - Many states do not have the necessary voting equipment in place to conduct these risk-limiting audits. In order to comply with the audit requirements, states and localities would be required to purchase new equipment.
- Likewise, the Act would amend HAVA to require states to have paper-based voting equipment to receive any future HAVA funding.
- The amended Act would not create a new federal bureaucracy in a new "Advisory Panel" as the original proposal did. Instead, it renames and expands a current EAC advisory panel to the "Technical Advisory Board."
    - While this is an improvement, it still provides no check and balances over the "Technical Advisory Board" or oversight of the board by the EAC (except for review of the guidelines under a short deadline). The EAC is a bipartisan panel that represents state and local election officials.
- The EAC should have more time to improve any voluntary guidelines with advice and recommendations of the local election officials in the Standards Boards.
    - The amended Act only gives the EAC 30 days to review new guidelines.

- The new Technical Advisory Board should not have singular authority to develop standards for the rest of the country without the checks and balances of election officials and the bipartisan EAC. Election officials should be an integral part of this process, not the pushed to the sidelines.

General Concerns about Federal Regulation of Election Administration and Cybersecurity

- The Secure Elections Act would further shift control of election administration from the states towards the federal government through the creation of federal cybersecurity standards. This would further standardize election systems around the country, which actually makes them more vulnerable to cyberattacks.
  - The cybersecurity of voter registration systems are currently protected by the nation's executive branch agencies and local governments.
  - The decentralized nature of our election systems and the wide variety of systems and procedures used around the country are the greatest protection against mass election hacking or tampering.
  - Standards developed by one federal agency for election purposes interferes with the flexibility provided to states in protecting all agencies.
- While protecting the cybersecurity of election processes is vitally important, states and localities are already doing this essential work.
  - States and localities have been establishing, planning, and implementing procedures to protect the security of elections long before it was in the national spotlight.
  - States and localities have physical and electronic laws and procedures for protecting the security of election systems.
    - States routinely handle sensitive information, such as identifying information through the DMV and medical information through Medicare and Medicaid.
    - Suggestions by the mainstream media, liberals, and federal government officials that states are incompetent in handling sensitive or important data are without merit. They undermine public confidence in election officials and election results and display a very Washington-esque disdain for the hard work and competence of the rest of the country.
  - While the federal government certainly has help and resources to offer, such help should be offered on a voluntary basis without regulatory "strings" attached.
- The rush to regulate at the federal level is in response to inaccurate reporting regarding what actually occurred in 2016.
- There is no evidence that a single vote or voter registration record was changed in the 2016 election. This is the extent of the known election cybersecurity incidents in 2016:
  - Before the 2016 election, Illinois' voter registration system was hacked, but no records were changed.
  - Some election official access credentials were obtained in Arizona and at the EAC, but likewise, no records were changed.
  - There were attempts to access other systems, many of which were "scans" to assess system security that systems deflect on a daily basis and some of which were focused at other, non-election state systems.