Strengthening Election Cybersecurity to Uphold Respect for Elections through Independent Testing (SECURE IT) Act

As the American people cast their ballots across the United States, their confidence in the value of their vote relies on the security of our election infrastructure. This infrastructure includes voting systems that enable and assist in the voting process across the country. Cybersecurity of these voting systems continues to be an important part of executing safe, secure, accessible, and transparent elections.

One important part of security testing is penetration testing - a method that enables researchers to search for vulnerabilities in a system. Current U.S. regulations under the Help America Vote Act of 2002 (HAVA) require the Elections Assistance Commission (EAC) to provide for the testing and certification, decertification, and recertification of voting system hardware and software by accredited laboratories. However, HAVA does not explicitly require penetration testing of voting systems.

To ensure the integrity of the voting process the SECURE IT Act addresses this issue by directing the EAC to require penetration testing as part of its certification process and to stand up a voluntary coordinated vulnerability disclosure program that will give independent researchers the chance to examine election systems for cybersecurity vulnerabilities.

Summary:

- Penetration Testing Requirement:
  - The bill directs the EAC to require cybersecurity penetration testing in order for a voting system to be certified.
  - The bill directs the EAC and the National Institute of Standards and Technology (NIST) to accredit entities that can perform penetration testing to fulfill the requirement described above.
- Voluntary Vulnerability Disclosure Program:
  - The bill directs the EAC to create a voluntary Coordinated Vulnerability Disclosure Program for election systems.
  - Under this program, vetted researchers would be given access to voting systems voluntarily provided by manufacturers for this purpose.
  - Researchers who discover vulnerabilities would disclose them to the manufacturer and EAC. Otherwise the researcher must keep the vulnerability confidential for 180 days, which is enough time for the manufacturer to create and promulgate a fix.
  - After the 180-day confidentiality period is over, the vulnerability will be included in the database of Common Vulnerabilities and Exposures.