ELECTION SECURITY ACT

As Introduced on February 14, 2018
by Reps. Bennie G. Thompson and Robert A. Brady and co-sponsored by
Reps. Zoe Lofgren, James R. Langevin, Cedric L. Richmond, and Val Demings

A product of oversight and outreach by the CONGRESSIONAL TASK FORCE ON ELECTION SECURITY, this bill addresses the lessons learned from the 2016 election about the risks to election infrastructure by prioritizing critical assistance to States and election administrators to protect their systems. Below is a summary of the key provisions.

Authorizes a $1 billion Election Assistance Commission (EAC) grant program to assist in securing election infrastructure.

Election officials can use this grant provided to replace aging voting machines with voter-marked paper ballot voting systems. Additionally, States can use these grants to help cover the costs of hiring IT staff, cybersecurity training, security and risk vulnerability assessments, and other steps to secure election infrastructure.

Provides States with sustainment funding to help maintain election infrastructure.

Seeks to ensure States can maintain security gains by providing each State with $1 per voter who participated in the most recent election to maintain election security.

Establishes a $20 million grant program for States to use in implementing risk-limiting audits.

Establishes a new $20 million grant program for States to access risk-limiting audits, a critical tool to ensuring the integrity of elections. These audits, which involve hand counting a certain number of ballots and using statistical methods to determine the accuracy of the original vote tally, are effective at detecting any incorrect election outcomes, whether caused by a cyberattack or something more mundane like a programming error.

Directs the Department of Homeland Security (DHS) to expand assistance to chief State election officials.

Requires DHS to expedite security clearances for State election officials in order to provide timely threat information and commence a security risk and vulnerability of a State's election systems within 90 days of receiving the request.

Requires Director of National Intelligence (DNI) to conduct regular threat assessments.

At least 180 days prior to a general election, the DNI would be required to complete a full-scope assessment of threats to election infrastructure.

Enhances protections for U.S. democratic institutions.

Directs the President, within a year of enactment, to issue a national strategy to protect U.S. democratic institutions against cyber attacks, influence operations, disinformation campaigns, and other activities that could undermine the security and integrity of such institutions. Additionally, it directs the establishment of a bipartisan commission to develop recommendations, drawing upon lessons learned from European allies, to counter such efforts.

Fosters accountability for election technology vendors.

Limit State expenditures on goods and services with grant monies provided under this Act to purchases from "qualified election infrastructure vendors"; EAC, in coordination with DHS, establishes the criteria for achieving such status, which includes maintaining IT infrastructure in a manner consistent with the best practices provided by EAC and DHS and agreeing to report any known or suspected security incidents involving election infrastructure. Additionally, it creates a certification program for voter registration software.

Creates a new DHS election infrastructure innovation grant program.

Authorizes $6.25 million annually, for DHS to award grants for research and development on improving the security, quality, reliability, accuracy, accessibility and affordability of election infrastructure.