U.S. HOUSE OF REPRESENTATIVES COMMITTEE ON
SCIENCE, SPACE, & TECHNOLOGY
Opening Statement

Chairwoman Haley Stevens (D-MI)
of the Subcommittee on Research and Technology

Joint Subcommittee Hearing:
Election Security: Voting Technology Vulnerabilities
Tuesday, June 25, 2019

Good afternoon and welcome to this hearing to review U.S. election security and voting technology vulnerabilities. I look forward to hearing testimony from our distinguished panel of witnesses on this important topic.

The elections of 2016 showed us how vulnerable our election infrastructure can be to foreign adversaries who interfere in the very foundation of our democratic process and began a national conversation on the security and integrity of elections. Most election authority rests with the states. However, Congress created a federal role in election administration and security with the Help America Vote Act of 2002, known as HAVA. Under HAVA, the National Institute of Standards and Technology, NIST, was tasked with providing technical assistance and research to inform the development of voluntary voting systems guidelines to be recommended to the Election Assistance Commission.

HAVA provided hundreds of millions of dollars to states to buy new voting equipment, and some of those old machines are still in use today. Further, states are not required to implement the voluntary voting system guidelines in the purchase of new voting machines. Only 38 states and the District of Columbia use some part of the federal testing and certification program for purchasing new voting equipment.

With more than 10,000 election jurisdictions in the United States, there is no one size fits all solution to election administration and security, but these guidelines are intended to have broad application. In addition, most election administrators are well intentioned but unfortunately lack the resources, awareness, and technical expertise to implement the vital security needs of today. At the time of HAVA, voting technology was assumed to mean only the voting machine itself. Today, depending on the jurisdiction, a voter may be able to register online to vote and have their name and address confirmed through an internet-connected electronic poll book (or e-poll book) at their polling site, in addition to casting their vote on an electronic machine.

Unfortunately, many Americans still cast their vote on machines with no paper record. I know we will hear from our experts today that, with all of the conveniences that the internet and 21st century technology provide, paper ballots are still the most secure. But even if we implement paper records everywhere, we are still left with the new security challenges posed with online registration and e-poll books. In fact, every point of internet connectivity in the election system, including software development and updating, introduces a vulnerability. Security must be a priority at every step of our cherished democratic process.

Last year, the National Academies issued a consensus study report titled, “Securing the Vote – Protecting American Democracy.” This report included several recommendations for improving elections security, including the need for national standards for e-poll books, voter registration databases, ballot handling procedures, and audits. Finally, the report included a strong statement that the federal government has a responsibility to invest in research to protect the integrity of elections. I couldn’t agree more, and am glad to know that in addition to NIST, the National Science Foundation carries out computer science and social science research that could be applicable to election systems. However, there needs to be more coordination and a more robust dedication of research dollars for this purpose.

The 2020 elections are not far away, I look forward to our witnesses’ insight on the Academies’ report and other important recommendations for actions this Committee can take to help.
Thank you and I yield back.