Testimony of David J. Becker

Executive Director, Center for Election Innovation & Research

Before the House Committee on Science, Space, & Technology

September 13, 2016

Good morning and thank you for the opportunity to testify today on the important issue of the security of our election system. My name is David Becker, and I am the Executive Director of the Center for Election Innovation & Research, a non-profit working in partnership with election officials and technology leaders to improve our system of elections.

My experience in elections goes back about two decades, starting with a seven-year stint as a senior trial attorney with the Voting Section of the Department of Justice, working in both the Clinton and George W. Bush administrations. While there, I litigated and enforced federal voting laws including the Voting Rights Act, the National Voter Registration Act, the Help America Vote Act, and the Uniformed and Overseas Citizens Absentee Voting Act.

I then served for several years as the director of the election initiatives program at The Pew Charitable Trusts where I oversaw efforts to use technology to improve the efficiency and security of elections. While there, I led the following initiatives:

- The Voting Information Project, where partnering with Google and other technology companies, we successfully delivered accurate election information to tens of millions of voters across the country, including millions in 2016 alone;
- Successful efforts to expand online voter registration, which has proven to be cost-effective and convenient, from two states in 2008 to over 30 states today;
- Helped found the Electronic Registration Information Center (ERIC), a sophisticated data center with over 20 member states that helps them keep their voter rolls up-to-date, and which so far has helped those states identify over 4 million out-of-date voter records and register almost 1 million new voters;
- Research that brought to light the difficulty military and overseas voters have, which led to the passage of the Military and Overseas Voter Empowerment Act in 2010.

During my time working in elections, I have observed dozens of elections in hundreds of polling places, and had the opportunity to visit many state and local election offices all over the country. In that capacity, I've learned much about the systems the states and counties have in place, and the security processes election professionals employ.

As an initial matter, we should be clear about the election systems in place, what they each do, and what, if any, relative vulnerabilities might exist. Voter registration databases are a key election system and have been in the news a lot recently. As you are aware, there was a breach of the Illinois voter registration database, where personal data from several thousand voter records were accessed. In Arizona, it appears the state successfully detected an attempted hack of their state voter registration database and prevented access of any private data. In both cases, initial investigation suggests no voter data was changed, the voter registration lists remained intact, with the primary goal of the hack being to

access personal data likely for purposes related to identity theft, rather than to manipulate the voter lists themselves. While we should continue to be vigilant about these centralized databases, to my knowledge, every state creates a regular backup of their voter registration lists – in most states on a daily basis – so that should anything go wrong with the databases themselves, the list could be reconstructed easily and quickly. It isn't impossible that the voter lists could be the target of an attack, but those lists are usually closed weeks before the election, with backup copies of the lists available in hardcopy and digitally should any mischief take place.

And while there have also been concerns expressed about the hack of the Democratic National Committee email system, that system is completely different than the election systems in place. That was an attack on a centralized email server, in a non-governmental entity, which bears no analogy to the highly-regulated systems in place in the states to administer elections.

The voting systems include paper ballots or electronic devices on which votes are cast, and include vote tabulation equipment, and with regard to those systems I can say that, while no system is 100 percent hack-proof, elections in this country are secure, perhaps as secure as they've ever been, and that voters should have confidence that their votes will be counted and counted accurately.

There are four primary reasons that voters should feel confident in our election system:

First, our election system is highly decentralized. Each state governs the administration of elections independently, and within each state, there are many individual election jurisdictions – counties, towns, and the like, totaling approximately 10,000 nationwide – that actually administer those elections. Even within many states, counties use different systems and dozens of different technologies to conduct elections. And within those thousands of election jurisdictions, there are well over 100,000 Election Day precincts and polling places where ballots are cast and collected. And that is just on Election Day, not taking into account the thousands of early voting sites, and tens of millions of paper mail ballots that will be utilized this November. Thus, there isn't a single or concentrated point of entry for a hacker. Rather, there are thousands of points a hacker would have to successfully navigate to manipulate the results of a national election.

Second, voting machines are kept secure. These machines are subjected to rigorous protocols for chain of custody and testing in every jurisdiction. Machines are held under lock and key with additional protections in place to ensure that nobody without proper credentials can access the devices. It is exceedingly difficult to gain unauthorized access to even one of these machines, and nearly impossible to gain access to more than one. Prior to every election – not just federal elections, but every time the equipment is used - these machines go through a series of tests called logic and accuracy tests to confirm that they are working as intended, recording and tabulating votes accurately. These tests are open to the public and entirely transparent, so everyone can observe; some jurisdictions even use social media to make sure that their voters can witness the process.

Third, unlike voter registration databases or email systems, I know of no jurisdiction where voting machines are connected to the internet. This makes it nearly impossible for a remote hacker, whether in Moscow, Russia or Moscow, Idaho, to access the equipment and plant malicious code or otherwise hack the system. Voting machines are kept secured, connected to nothing – not even power - until they are tested and used, and then they are under constant observation. Without connectivity, it would require a hacker to have unfettered physical access and enough time to sabotage one machine just to impact the

results on one device in one polling place. To manipulate election results on a state or national scale would require a conspiracy of literally hundreds of thousands, and for that massive conspiracy to go undetected.

Which brings us to the fourth reason. Even if hundreds of thousands of conspirators operated undetected on the diverse range of systems, defeating the testing and chain of custody protections in place, it would still have no effect on the vast majority of election results nationwide. That is because well over 75 percent of voters vote on paper ballots or on a device that creates a paper record. And in most states – 32 plus the District of Columbia, as of 2014 – there is a post-election audit requirement that mandates states match the paper record to the digital record, and if a discrepancy exists, recount the paper ballots for use as the official record. The states that require such an audit include the battleground states of Arizona, Colorado, Florida, Nevada, New Mexico, North Carolina, Ohio, Pennsylvania, Virginia, and Wisconsin, among others. So even if a grand conspiracy were viable, a post-election audit requirement would almost certainly discover it prior to election results becoming official, with the paper ballots then being used as the official ballot of record.

There has been a lot of hyperbole surrounding this election, but the processes in place to ensure the integrity of our election system should not become part of the political rhetoric. I've yet to meet an election official at the state or local level, Republican or Democrat or neither, who was not working as hard as possible to ensure that every election reflects the will of the people, even if the outcome differed from their own political interests. There are a few loudly seeking to sow distrust in the system, but there are far more working quietly and collaboratively, at the federal, state, and local level, to secure our voting systems and reassure voters that this election will accurately reflect voters' choices.

And voters can play a role as well, by attending pre-election logic and accuracy tests, and especially, volunteering to serve as poll workers to see the process first hand. Whether it is federal officials offering assistance and resources to the states, state and local officials sharing best practices, or citizens serving as poll workers, this cooperation and diligence will protect our elections in 2016 and safeguard future elections as well.