TESTIMONY OF DAVID J. BECKER

EXECUTIVE DIRECTOR, CENTER FOR ELECTION INNOVATION & RESEARCH

Pennsylvania House State Government Committee

October 15, 2018

Mr. Chair, and members of the committee, thank you for the invitation to testify before you today, about the important issue of election integrity and security. With voter confidence at risk, and foreign adversaries intent upon weakening democratic institutions, this issue is more important than ever.

My name is David Becker, and I am the Executive Director and founder of the Center for Election Innovation and Research. CEIR is an innovative nonprofit with a proven track record of working with election officials from around the country and from both sides of the aisle. We work to build voter trust and confidence, increase voter participation, and improve the efficiency of election administration.

Prior to founding CEIR, I led the elections team at the Pew Charitable Trusts for many years, and before that, I served as a trial attorney in the Voting Section of the Civil Rights Division of the U.S. Department of Justice under both the Clinton and W. Bush administrations. Overall, I have over two decades of experience working to improve the efficiency, security, and integrity of elections, in states across the political spectrum.

The good news is that voting in the United States, and Pennsylvania in particular, is easier, and more secure, than ever before. More voters than ever have an easier time registering to vote, voting with more options, and can be assured their vote will be counted properly. But we're going to need to keep improving to ensure security, integrity, and access for all voters, and Pennsylvania is on that path.

First, we know that foreign adversaries have attempted to attack our election infrastructure. The threat from Russia and perhaps others is real. Russia attempted to infiltrate voter registration databases in 2016, and while almost all of those efforts were unsuccessful – only the Illinois voter database was successfully breached, and no records were altered or deleted – our intelligence services and the Department of Homeland Security agree that the threat remains and we must be vigilant to secure our systems.

But while vigilance is important, we must also not be hysterical about potential vulnerabilities. In just the last few weeks, media reports have included claims that election officials are to blame if Russia attacks our election again, that voting systems are more vulnerable than ever, that nobody is trying to fix them. These claims are all demonstrably false, and there remains zero evidence that votes in any past U.S. election were interfered with or changed, despite substantial investigation. So I think it's important to note the tremendous progress that has been made since 2016.

Most election experts, including myself, advise that the best defense against interference with the vote itself, is to use paper ballots, with a robust audit of those ballots to ensure any mechanical count was accurate. We're close to that goal nationwide – already 80% of all U.S. voters can cast a paper ballot, the highest percentage of non-punch card paper ballot availability since computers were introduced to voting. Since 2016, the State of Virginia has moved to entirely paper, and other states like Delaware are

moving to paper right after 2018. And thanks to efforts from the Secretary of State's office, and local election officials, Pennsylvania is likely to have paper well before 2020, as will the other states who still use paperless systems.

A majority of states have audits of their paper ballots, and a growing number of states are leading the way to even more robust audits of their paper ballots. Wisconsin just reported a move towards very robust audits this year. Pennsylvania requires a small audit of ballots, but as it implements paper statewide, it may be advisable to consider a more significant routine random audit of ballots to ensure confidence in the outcome. My organization and others are working with states on helping them implement such audits.

Congress has stepped up with a one-time, $380 million appropriation to the states, including over $13 million for Pennsylvania. The state is using these funds to help the counties with better security protocols, as most of the states are.

All 50 states and over 1000 local election offices and the federal government are sharing information on potential election cyberthreats as never before, through and organization called the Election Infrastructure Information Sharing and Analysis Center, of EI-ISAC. The EI-ISAC didn't even exist until earlier this year, and already every state is participating. And Pennsylvania and virtually every other state has partnered with DHS to hold tabletop exercises simulating a variety of possible cyber-attacks to election infrastructure.

So voters should know that their votes will be counted, and counted accurately. But what about the one area where we know a vulnerability has been exploited – our voter databases. CEIR has worked with states on this important issue, and recently surveyed the states to determine whether states are adopting best practices for security of their voter lists. A majority of the states responded, though Pennsylvania did not. Our findings are that states have made significant progress, though further improvement is needed.

For instance, there are several security protocols we recommend, which can help prevent an attack on a voter database from occurring, detect any attempted intrusion, and if necessary, mitigate the effects of any successful infiltration. These recommendations include:

- Secure password requirements, requiring authorized users to use uncommon, sufficiently long and complex passwords, and to change them regularly;
- Multi-factor authentication, which requires an identifying factor other than a password to log in, such as a confirming text message, or use of a token which can generate a separate password;
- Regularly training voter registration database users, including county and local staff with access, to detect cyber threats, like phishing;
- Deploying tools like Albert sensors (in partnership with the Center for Internet Security and DHS), and other tools to consistently monitor for improper access to the voter database, including checking for things like unusual volume of activity, or activity originating in a foreign country;
- Use secure HTTPS for websites with sensitive information;

- Employ tools to prevent distributed denial-of-service (DDoS) attacks;
- Utilize email protection tools;
- Regular backups of the voter database, daily if possible. And regular tests of those backups so that the system can be restored quickly if necessary.

Based on our survey, it's clear that a significant majority of states are utilizing most of the recommended tools. Indeed, over 90% of voters live in jurisdictions protected by Albert sensors. However, there are areas for improvement. For instance, states can do better when it comes to implementing more secure password requirements and further adopting multi-factor authentication. As for Pennsylvania, I'm not aware of whether all these recommendations, and the others made in the report, are being followed, but knowing their approach to security, I think it's likely Pennsylvania is implementing most of these, and you can confirm directly with the Department of State.

Finally, I'd like to discuss one key area of election integrity, related to the voter database, and that's the accuracy of the voter lists themselves. Election officials from across the political spectrum agree that it's important that the voter lists are as accurate and up-to-date as possible, and represent only those who are eligible to vote.

States are doing better than ever before in meeting this goal, thanks to three key strategies which we recommend, all of which Pennsylvania has been at the leading edge in implementing.

First, online voter registration. This is a basic system that allows voter registration to enter the 21st century. Though there were only two states offering online voter registration ten years ago, now nearly 40 states do, including Pennsylvania, and it's only a matter of a few years before every voter can register to vote securely online, 24 hours a day, reducing the amount of paper to process, errors in data entry, and possible voter registration fraud.

Second, automating the motor voter process. When a citizen experiences a life event – a move, a name change, or coming of age – the agency they're most likely to tell first is motor vehicles. When motor vehicles can efficiently and effectively pass on information about new voters, or updates for existing voters, to election officials, the lists are more accurate and up-to-date. This should be a fully electronic process, eliminating paper, to maximize efficiency. Pennsylvania has been a national leader in modernizing its systems, and many other states are looking to Pennsylvania's model as they consider more automation.

Last, membership in the Electronic Registration Information Center, or ERIC. ERIC is a sophisticated data center, run by the states that choose to participate, that helps states improve the accuracy of America's voter rolls and increase access to voter registration for all eligible citizens. As of this summer, ERIC has helped its 24 member states, including Pennsylvania, identify over 7.2 million voters who moved within the state (but the voter record hadn't been updated), over 2.2 million voters who moved out of the state and were therefore no longer eligible to vote in that state, and over 220,000 voter records for individuals who had passed away since they last voted. All totaled, ERIC is responsible for correcting nearly 10 million voter records that were no longer accurate, since its inception in 2012.

Pennsylvania and other states have made great strides in election integrity in the last several years, but there is more work to be done, particularly in election cybersecurity. Election officials stand ready to

continue to make improvements, but they need resources. There is no finish line in cybersecurity – as we improve our defenses, those who would seek to undermine our democracy will improve their attack capabilities. Therefore, election officials will need a more regular stream of funding to ensure they can continue the progress in securing our election systems. Funds are needed to purchase new technology, and hire and train staff. I am hopeful that the states will step up to provide these needed resources, perhaps in partnership with Congress, to ensure that voters can have confidence that their votes will count.

Thank you, and I'd be happy to answer any questions.