U.S. Senate Committee on Rules and Administration

Hearing on Election Security Preparations: A State and Local Perspective

Wednesday, June 20, 2018

Good morning Mr. Chairman, Mr. Vice Chairman and distinguished members of the committee.

Thank you for the opportunity to offer testimony this morning.

My name is Shane Schoeller. I am honored to serve as County Clerk in Greene County, Missouri. Greene County is the fourth largest county in our state and has an estimated population of 288,072 and over 189,000 registered voters.

The county clerk in each county of our state is responsible for several county organizational functions that include tax administration, secretary to the board of equalization, licensing and notary issuance, county payroll and benefits administration, retention and archival of county records, voter registration, and election administration. The most visible role our office performs is clearly election administration.

I firmly believe that the foundation of public confidence in our local, state and federal government is anchored in the conduct of impartial, fair and honest elections. When an election outcome is cast in doubt, confidence quickly begins to erode and potentially impacts voter turnout in future elections. In short, this means there is no room for error in the work that we do leading up to election day. It is a duty that my fellow county clerks and election directors across our state take seriously as we work tirelessly to ensure accuracy in the correct ballot being given to each voter and then the results of their cast ballots being correctly tabulated.

It is important in the context of this testimony today to recognize that each state is unique in how their elections are administered at the local level and I realize that some of the perspective I share today will be unique to Missouri. What is not unique though, is that like Missouri, many election authorities state-by-state are tasked with several administrative duties beyond just election administration and they do so with limited budgets and personnel.

While there are challenges as I just mentioned, the advantage in keeping election administration local is that it is clearly better positioned to be more efficient and effective in carrying out these duties and responsibilities to its citizens than state and federal government could provide. This effort in large part is decentralized and yet it all

comes together during each November General Election as citizens across the country await the announcement of election results from their local election authorities that night as polls close and votes are tabulated.

It is most unique, in that it is by and large a very shared responsibility in terms of providing election results on election night and yet there is a real difference state by state in the election laws and procedures for how the election will be conducted. This includes the preparation duties necessary to conduct the election and the method of voting on election day. Then after the election there are real differences in the post-auditing and verification procedures prior to certifying the election results state by state. This separation and decentralization of election administration is an advantage in protecting against a broad-based systemic cyber-attack on our elections from a foreign enemy who may one day attempt to alter the election outcome through a cyber-attack.

The advantage of being decentralized for local election officials is also a challenge as it relates to cybersecurity threats. This is especially true in regards to electronic voter registration data and the electronic tabulation of election results on election night. It is fair to say that the majority of county clerks in the rural areas of Missouri are depending on the efforts of their election service providers who provide their voting equipment services, the Secretary of State's (SOS) office and the coordinated efforts of the Department of Homeland Security (DHS) and the Election Assistance Commission (EAC) to be their firewall for protection against incoming cybersecurity threats.

I am fortunate to have the added benefit to work closely with our information systems (IS) team in my county as we learn about potential cybersecurity threats via the EAC, the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC), and the Multi-State Information Sharing and Analysis Center (MS-ISAC). Our IS team with this information works tirelessly to protect our county and my office through a layered security approach to defend against external cyber security threats. Not all election authorities have access to a team dedicated to protecting them from external cyber security threats and that is an important point that cannot be underestimated as we continue preparing for the November General Election.

I currently serve on the Advisory Board for the EAC. I appreciate their continued and increasing coordinated efforts to provide critical information on security preparedness to state and local election officials. Their work with DHS and the National Association of Secretaries of State (NASS) is welcome. I am optimistic that these good efforts will continue and be further enhanced through one of the provisions within the Secure Elections Act should it be passed and signed into law. This provision would change the "Technical Guidelines Development Committee" to the "Technical Advisory Board" and would include cybersecurity experts as part of the board. I believe changes like this are

needed to build on the current information sharing that was not in place prior to the 2016 election.

As a local election official, I would like to see further efforts made at the state and federal level to continue improving how cybersecurity information is shared to local election officials in a common sense and productive way. As I mentioned earlier, it is not uncommon for a local election official to be overtasked and under resourced to adequately oversee all the various administrative duties of the office. To this point, I recommended during our most recent EAC Advisory Board meeting in Miami earlier this year, that the EAC consider setting up an information network to help disperse important information to a designated contact in each state who is known by local elections officials. As issues arise that need to be quickly addressed, there is a greater likelihood that the information will be paid attention to if the email recipient personally knows who the sender of the email is coming from. The value of the work performed by the EAC, DHS, NASS, MS-ISAC and EI-ISAC is considerably less in its impact if the information is not adequately shared in a logical and productive way.

I do want to address one area of concern in the Secure Elections Act and that is on page 23, lines three, four and five. It says, "each election result is determined by tabulating marked ballots (hand or device)." I strongly recommend for post-election auditing purposes that it state "marked paper ballots."

Earlier this year we purchased a new voting system for our county that is paper based. To help eliminate any unrealized biases towards one voting system over another I formed an Election Advisory Board that represented a broad cross-section of the voters we serve. Their perspective was critical as we went through the selection process and there was never any disagreement by any member of the board that the voting equipment purchased must be paper based. I believe the opportunity for fraud in an "electronic ballot casting system" that does not have a paper trail is too great. I do not see, but am open to being shown, how an impeccable and fair standard of accountability could be implemented to ensure the outcome is exactly as the voters voted when an election is conducted without any paper records.

For example, we follow both state statute and the Missouri Code of State Regulations in pre-testing and post-testing all voting equipment used on election day. Paper ballot test decks are created and manually counted by each bi-partisan certification team prior to the testing that is performed on each voting machine with the test decks and it is all open to the public. Then after the election, there is a manual count of the voted paper ballots based on a random drawing by a bipartisan team from all voting precincts on election day. Being able to share with voters that the paper ballots they cast were randomly selected to be recounted by hand was critical to helping earn their confidence that the certified election results in the 2016 General Election were accurate. It is

important to add when Secretary Kirstjen Nielsen of the Department of Homeland Security testified to the Senate Intelligence Committee back in March of this year, she stated the importance of using paper ballots as vital to the safeguarding and protecting the integrity of electronically tabulated election results.

An area of concern that has received less focus, but cannot be underestimated, is the possibility of an attempted cyber-attack to alter electronic-based voter rosters that are now commonly used in place of paper-based voter rosters when checking in voters on election day. The benefits of checking in a voter on an iPad or tablet-based check-in system have been enormous, as we can now scan in a voter's identification information through their voter registration card or their driver's license. Alphabetically organized check-in lines have been eliminated, thereby reducing the number of election judges needed to check-in voters. It is a convenience that voters really appreciate as they see wait times reduced.

This convenience can quickly evaporate and become the source of real issues on election day if either the statewide voter registration system is compromised or the election service provider that provides both the hardware and software needed for an electronic roster is compromised in some way. I can assure you that it will not end well with voters who have not voted being informed on the day of the election that they already voted, or their name cannot be found to check them in to vote. I am sure you would agree with me that this is the perfect recipe for voters to become very angry and for real chaos to ensue. This scenario occurred on a small-scale level in Durham County, North Carolina, in November of 2016 and it cannot be ignored.

As each of you well know, there is little if any grace given in performing the duties of public office when problems or mistakes occur like I just described. It is understandable to a large degree, but it cannot be expected that a smaller third-class county would have the necessary resources to defend itself against a cyber-attack to their systems. When you realize that entities like the Department of Defense and major Fortune 500 companies have been compromised by cyber-attacks, both of which have unlimited resources as compared to almost any size local government, it is evident our local election officials who have no resources available to monitor and prevent incoming cyber-attacks need outside help from the DHS and the SOS to help them withstand future cyber-attacks on their voter registration data and voting equipment that tabulates election night results.

I recommend that DHS, in coordination with our secretaries of state, assess state by state where the weakest vulnerabilities are county by county. Based on the information learned, I believe necessary cyber defense protection can be provided where it is needed to help ensure the integrity of our elections this November will be protected before it is too late. To that end I am very pleased that in our state, Secretary Ashcroft is setting up of regional meetings across the state with election authorities to begin these

conversations he is calling Cyber Chats. The purpose will be to begin discussing now the importance of cybersecurity protection and the sharing of best practices in cybersecurity defense as we plan for November.

As I conclude my remarks, I want to emphasize that I firmly believe that elections are the cornerstone of our freedom and we must all work together to protect that freedom and its integrity every time a voter cast his or her ballot. I believe we are up to the task if we do it together.

Thank you for holding today's committee hearing to assess the state of election security preparation in our nation as we prepare for this November, and I look forward to answering the Committee's questions.