S. HRG. 115–648

ELECTION SECURITY PREPARATIONS

HEARINGS

BEFORE THE

COMMITTEE ON RULES AND ADMINISTRATION UNITED STATES SENATE

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

JUNE 20, 2018 AND JULY 11, 2018

Printed for the use of the Committee on Rules and Administration

Available via the World Wide Web: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE
35–266 WASHINGTON : 2019

COMMITTEE ON RULES AND ADMINISTRATION

SECOND SESSION

ROY BLUNT, Missouri, *Chairman*

MITCH McCONNELL, Kentucky	AMY KLOBUCHAR, Minnesota
LAMAR ALEXANDER, Tennessee	DIANNE FEINSTEIN, California
PAT ROBERTS, Kansas	CHARLES E. SCHUMER, New York
RICHARD SHELBY, Alabama	RICHARD J. DURBIN, Illinois
TED CRUZ, Texas	TOM UDALL, New Mexico
SHELLEY MOORE CAPITO, West Virginia	MARK R. WARNER, Virginia
ROGER WICKER, Mississippi	PATRICK J. LEAHY, Vermont
DEB FISCHER, Nebraska	ANGUS S. KING, JR., Maine
CINDY HYDE-SMITH, Mississippi	CATHERINE CORTEZ MASTO, Nevada

FITZHUGH ELDER IV, *Staff Director*
ELIZABETH PELUSO, *Democratic Staff Director*

Note: Archived webcasts of all hearings and an electronic version of this report are available at *http://rules.senate.gov*.

C O N T E N T S

Page

July 11, 2018

HEARING—ELECTION SECURITY PREPARATIONS: FEDERAL AND VENDOR PERSPECTIVES

OPENING STATEMENT OF:

PANEL I

PANEL II

PREPARED STATEMENTS OF:

MATERIALS SUBMITTED FOR THE RECORD:

QUESTIONS SUBMITTED FOR THE RECORD:

ELECTION SECURITY PREPARATIONS: A STATE AND LOCAL PERSPECTIVE

WEDNESDAY, JUNE 20, 2018

UNITED STATES SENATE,
COMMITTEE ON RULES AND ADMINISTRATION,
Washington, DC.

The committee met, pursuant to notice, at 10:57 a.m., in Room SR–301, Russell Senate Office Building, Hon. Roy Blunt, Chairman of the committee, presiding.

Present: Senators Blunt, Fischer, Klobuchar, Durbin, Udall, and Cortez Masto.

OPENING STATEMENT OF HONORABLE ROY BLUNT, CHAIRMAN, A U.S. SENATOR FROM THE STATE OF MISSOURI

Chairman BLUNT. The Committee on Rules and Administration will come to order.

Glad our witnesses are here. Glad you had the patience that we needed today to get two votes done on the floor. I am particularly grateful that my fellow Missourians are here—Secretary of State Jay Ashcroft, and in the next panel is County Clerk Shane Schoeller from my home county—and both of them having to hold a job that I once held. It is particularly good to see you here and the rest of you on the panel.

As we begin our review of Federal elections, Senator Klobuchar and I are in agreement that the best starting point is to start with you. The best starting point is to start with state and local officials who, through the history of the country, have been responsible for election administration, and they are responsible to the people that choose them to do that job to see that it is done well.

Clearly, elections are the keystone of democracy, and they are dependent on the efforts of county officials, of election directors, of secretaries of state, and many others. On election day, they are dependent on lots of people who essentially figure out how to volunteer for their job at the polling place.

During the 2016 election cycle, state and local election officials were tested like they haven't been before by cyberattacks, and we anticipate that these attempts will continue, and attempts to interfere with the process will continue. We want to be sure that we are doing what we can to help you thwart these attempts. State and local governments need access to timely and actionable information and technical assistance when they need it.

One of our goals today is to find out more about the information sharing that is occurring between Federal, state, and local officials and to learn more about your concerns and your thoughts on that.

In January 2017, the Department of Homeland Security designated our country's election infrastructure to be critical infrastructure. This designation began the formalization of information sharing and collaboration among state, local, and Federal governments through the creation of a Government Coordinating Council. Some of our witnesses this day are already sitting on that newly formed council.

More recently, in the 2018 omnibus, Congress appropriated right at $380 million to the U.S. Election Assistance Commission to help states enhance their election infrastructure. As of this week, 38 states have requested $250 million of that money, and about $150 million of it has already been disbursed to the states.

Finally, the attempts to influence the 2016 election have spurred many calls for additional laws. I remain open to learning more about where those gaps are and how we approach those gaps in a way that continues to let local officials do their job, but be sure that there is maximum confidence in what happens on election day.

Glad all of you are here. Certainly, it is a pleasure for Senator Klobuchar and I to get to work together on this and particularly for me to get to work with her. We have had a long history of working together, but just this year starting to be the top two individuals on this committee.

Senator Klobuchar, I would recognize you for your opening statements.

OPENING STATEMENT OF HONORABLE AMY KLOBUCHAR, A UNITED STATES SENATOR FROM THE STATE OF MINNESOTA

Senator KLOBUCHAR. Well, thank you very much, Chairman Blunt.

This committee's jurisdiction is clear. We have jurisdiction over Federal elections, and obviously, there has been a lot of other committees looking into this issue as part of investigations, including Judiciary on which I serve. But in the end, if we want to get something done and make some changes, I think it is really important that this committee weigh in, and a lot of the bills will actually be going through this committee.

According to the Department of Homeland Security, you all know this, 21 states' election systems were attempted to be hacked into by a foreign country—that would be Russia—and this was established not just by the intelligence heads under President Obama, but also by the intelligence heads in sworn testimony under President Trump. I think it was former Senator Coats, now the Director of Intelligence for our country, that said he believes that they are going to get bolder in the next election.

I don't think we need to get more direction than that to know that we must act. Secretary of State Pompeo said when he was CIA Director that he has "every expectation" that Russia will target the U.S. midterm elections. Those are the facts from our intelligence forces, and rather than just admire this problem, we have to look at what we can do to make things better.

One of the things that we have done, and I appreciate the input from the secretary of states, including my own, Steve Simon, who is here—thank you. I will note that Minnesota has the highest election turnout in the country nearly every year, including last year.

Oh, excuse me, Illinois.

[Laughter.]

Senator KLOBUCHAR. We are continuing that record, and a lot of that is the election laws that we have in place for same-day registration and other things that have made that possible.

But our subject today is how to protect our elections, how to make them more secure with the facts that we have, that we allow our state election officials to get information in real time about hacks across the country because, you know, hack us once, shame on them. Hack us twice, shame on us if we don't do anything about it. Because we know it happened, and we know it will happen again. In fact, in Illinois, they got as close as the voter data information.

We have a bill, Senator Lankford and I—along with Senator Harris and Graham and Warner and Burr, Heinrich and Collins—it is a bipartisan bill called the Secure Elections Act, and we have been working to make changes to it along the way and introduce it as amendment. But it really does four things.

First of all, improves information sharing between local election officials, cybersecurity experts, and national security personnel.

Second, providing for development and maintenance of cybersecurity best practices. We all know I think there is five states that don't have back-up paper ballots, and then there is something like nine more that have partial back-up paper ballots. While we are not mandating what each state does, and we do not want each state to have the exact same election equipment, we think that would be a problem and would actually lend—it could potentially lend itself to more break-ins, we think it is really important that we have some floor and standards that we set that, given what we know, I don't think we would be doing our democracy any good if we didn't share that and we didn't put in some floors.

Third, the bill will promote better auditing. Our elections use the paper back-up systems, which I mentioned.

Finally, it is focused on providing election officials with much-needed resources. As you all know, we were able to get $380 million to be immediately distributed to the state—not play money, money that is going out right now to states across the country based on population. We didn't have some complicated grant process that would have slowed things down. The money went directly to state election officials as long as the State legislature authorizes it to get accepted and get to work to update their systems.

That is what we have been focused on, and we want to thank you for your involvement, and I think we know what the facts are and what the evidence is. I will end with this, a reminder of what is at stake.

In 1923, years before Sputnik and the Internet, Joseph Stalin, then General Secretary of the Soviet Communists, was asked about a vote in the Central Committee of his party. Stalin was unconcerned about the vote. After all, he explained that who voted was completely unimportant. What was extraordinarily important, he said, was who would count the votes.

Now 95 years later, those words echo in this room as we realize that this country or they would say not the people, but the leader

of this country, Vladimir Putin, was once again really trying to influence who counts the votes and how the votes are counted by attempting to hack into our systems. We cannot have that happen. I don't care if we are a Democrat, Republican. I don't care who you are for in the Presidential race or who you are for in these Senate races. This is really about the integrity of our democracy.

Thank you, Senator Blunt.

Chairman BLUNT. Thank you, Senator Klobuchar.

Again, I want to thank the witnesses for joining us today. Unfortunately, weather and a flight cancellation made it impossible for Secretary Lawson's attendance today, but we are glad that she tried to come, and we are glad you are here.

Let us turn to our panel. First, Secretary of State Ashcroft from Missouri will start, and then Secretary Condos of Vermont, Secretary Simon of Minnesota, and finally, Mr. Masterson of the Department of Homeland Security. We have your comments for the record. You can use as much or little of that as you want to, and we will have it for the record no matter what.

Secretary Ashcroft, we are glad all of you are here and eager for you to start.

OPENING STATEMENT OF JOHN ASHCROFT, MISSOURI SECRETARY OF STATE

Mr. ASHCROFT. Thank you, Chairman Blunt, Ranking Member Klobuchar, and distinguished committee members, for the opportunity to join you here today for this important discussion regarding the security of our elections.

My name, as mentioned, is John Ashcroft, and it is my distinct privilege and honor to serve as the 40th Secretary of State for the great people of the State of Missouri. As was already noted, this is an office administered at one time by the chairman of this committee.

I decided to run for Secretary of State because of my four children. My goal was to ensure their voices and those of future generations would continue to be heard at the ballot box. One of the priorities of my campaign was to enact legislation that both increased the security of our votes and made sure that every registered voter could vote. Simply put, in Missouri, if you are registered, you can vote, and your vote will count.

Elections are the bedrock of our democratic republic, as they are how we the people consent to be governed. The integrity of these elections is of the utmost importance, every day when I go to my office in Jefferson City, and I know my fellow election officials across this country share that same concern and dedication.

I welcome today's conversation to talk about election security preparations, but before we move forward, we should briefly look back to the impetus of why we are all here today—allegations that outside actors threatened the integrity of our elections during the 2016 election cycle.

While these are serious allegations, it is vitally important to understand that after 2 years of investigation, there is no credible—and I could strike "credible" and just put "evidence." There is no evidence that these incidents caused a single vote or a single voter registration to be improperly altered during the 2016 election cycle.

It was not our votes or our election systems that were hacked. It was the people's perception of our elections.

Secondly, every reported cyber incident in 2016 involving state election systems was first detected by state election authorities, not the Federal Government. In each case, election authorities brought the incident to the attention of Federal authorities, not the other way around.

This is not to say that our elections are perfect, that there was no fraud, that there were no unlawful corruptions of votes or vote totals. The evidence indicates that voter fraud is an exponentially greater threat than hacking of our election equipment.

In 2010, well before elections being altered rose to the forefront of the public conversation, there was a race for the Missouri house in Missouri that was decided by one vote. Yes, one vote. Election authorities conclusively determined in that election that there were two voters, who also happened to be family members of the victorious candidate, who voted illegally. Despite the fact that the candidate's relatives admitted, admitted in a court of law, pled guilty to illegally voting, their nephew now serves in the Missouri legislature.

Consequently, moving forward, any meaningful enhancement to election security must take a comprehensive approach to ensure that every legally registered voter is allowed to vote and that their vote is not diluted by any sort of voter fraud, malfeasance, or ineptitude. Moreover, we must avoid knee-jerk reactions that would give voters a false sense of security.

Steps must be taken to improve communication between Federal agencies and states regarding cyber threats and election security. States have and will continue to work with Federal agencies, regardless of any new legislation. However, any new mandates must remedy the failure of Federal agencies to communicate and work with local election authorities.

As one example, since 2012, the National Association of Secretaries of State has passed multiple times a resolution calling on the Federal Government to meet its statutory obligations to share information with state election officials. While we wish to continue—state election officials wish to continue to work in partnership with Federal agencies, and one way in which we have done that, as states have teamed up in September, we will be having a National Election Security Summit in St. Louis, Missouri, and we have requested Federal officials, including the Secretary of DHS, to join us, as state officials, vendors, technology experts, and local election officials get together to improve processes and make sure that people know that our elections are secure.

As important as this information sharing is, there are numerous other ways to protect our elections beyond information sharing. Proposed changes should recognize the value of allowing state election officials to remain in control of elections. I have learned that winning an election does not make you an elections expert any more than watching a Fourth of July celebration makes you a rocket scientist.

I will close by noting a certain irony. Just over 10 years ago, similar individuals were here in Washington, DC, explaining what happened in a Federal election, and we were told that the answer

was to go electronic, to put it all on a computer. Now we are back again.

With the utmost respect, I will continue to work and local officials will work with Government officials at the Federal level, but it takes us all working together and the expertise of individuals that have run elections before.

Thank you very much.

[The prepared statement of Mr. Ashcroft was submitted for the record.]

Chairman BLUNT. Thank you, Secretary Ashcroft.

Secretary Condos?

OPENING STATEMENT OF JIM CONDOS, VERMONT SECRETARY OF STATE

Mr. CONDOS. Good morning, Chairman Blunt, Ranking Member Klobuchar, and distinguished members of the committee.

My name is Jim Condos, and I am Vermont's 38th Secretary of State. I am also the President-elect of the nonpartisan National Association of Secretaries of State. In addition, I also serve as a member of the Department of Homeland Security's Election Infrastructure Subsector Government Coordinating Council, EIS-GCC.

On July 16, 2018, I will become the new NASS president, and I have every intention of continuing the positive work of current president, Secretary Connie Lawson of Indiana, and those that served before her. NASS is fortunate to have had and have leaders, outstanding leaders, and I am proud to be part of this association.

Thank you for the chance to appear before you today with my colleagues and for allowing us to address some of the things happening at the national level, some work specific to Vermont, and also my goals for NASS and the Election Infrastructure Governing Council.

Primary elections across this country are well underway with states administering elections in a secure, accurate, and fair manner. State and local election officials and Federal Government have worked very hard to create a productive relationship since the critical infrastructure designation for election systems in January 2017.

As you may know, NASS and its members raised many questions and expressed serious concerns about the potential Federal overreach into the administration of the elections—clearly, a state and local government responsibility. While we remain vigilant about possible Federal overreach, we will work together to ensure that the critical infrastructure designation functions in an effective way.

Thus, we have chosen to actively focus on improving communications between the states and the Federal Government and to achieve our shared goal of securing elections. In particular, we have utilized the Election Infrastructure Subsector Governing Council, which Secretary Lawson mentions also in her testimony, to open communication channels and guide future collaborative election security endeavors.

As I transition to the NASS president in less than a month, I will also take Secretary Lawson's place on the Executive Committee of the GCC. It is my objective to continue Secretary Lawson's vital work with this group on behalf of NASS.

In regards to specific state preparations for 2018 and beyond, I would like to thank you and your colleagues for appropriating the remaining Help America Vote Act funds to the states in the recent omnibus bill. We truly appreciate this money, and it will go a long way to helping states strengthen and improve their election systems.

While our upgrades to equipment and cybersecurity will be an ongoing challenge for many states, the Federal funding received will regrettably be insufficient to do all that we want or need. However, we are very grateful for the boost that these Federal funds provide us at this time.

In Vermont, we have already requested and received our $3 million grant of HAVA dollars from the U.S. Election Assistance Commission. By the way, the EAC has provided this in a very quick way. It is within 3 to 5 days of actually receiving our application, they are getting the money to us. I want to thank the EAC publicly for providing a simple and quick method of getting that money to us.

In regards to specific plans in using these new HAVA funds, in part our office in Vermont plans to implement prior to the 2018 primary two-factor authentication for all of our local clerks and our SOS staff to access our election management system. We have already conducted an additional round of penetration testing on our election management system by an independent vendor this spring and will do so at regular intervals going forward.

We also will follow the 2018 general election, and every general election going forward, with a robust audit of our election results using state-of-the-art auditing technology. This plan is in addition to what we are already currently doing, including mandatory election trainings to our Vermont municipal clerks, holding the cyber summit, which we named Defending Our Democracy. We convened state and local partners to inform Vermonters of our efforts, build confidence in the integrity, and those partners included the Department of Homeland Security, MS-ISAC from the Center of Internet Security, State Homeland Security Department of Public Safety, and of course, our town clerks.

Some of the acknowledged best practices that Vermont is using include paper ballot, post-election audits, no Internet, daily backup of our voter registration systems, daily monitoring of traffic to our site, blacklisting of known problems, periodic penetration tests, securing the human, and we have actually installed a real-time Albert monitor.

I will end by just thanking this committee again for inviting me and my peers to testify and for giving me the opportunity to speak about this important matter on behalf of NASS and Vermont. I look forward to answering your questions.

[The prepared statement of Mr. Condos was submitted for the record.]

Chairman BLUNT. Thank you, Secretary Condos.

Secretary Simon?

OPENING STATEMENT OF STEVE SIMON, MINNESOTA SECRETARY OF STATE

Mr. SIMON. Thank you, Chairman Blunt. Thank you, Ranking Member Klobuchar.

I really appreciate the opportunity to be with you here today. Thank you for your willingness to engage on this very important issue.

In my judgment, election security in general, and cybersecurity in particular, poses the number-one threat to the integrity of our elections, both nationwide and in the State of Minnesota. I have been on the job, this job now for 3 1/2 years, and I get asked once in a while—whether it is at a family gathering or someone I bump into on the street—what is your biggest surprise in the job? You have been there for a while now. What is it?

My answer is always the same. My biggest surprise as Secretary of State is the extent to which my time and energy and focus is spent on this cybersecurity issue or election security in general. It is something that came up to some people's minds quite suddenly in 2016. That was a big wake-up call, and that is now a central and essential part of the job.

The good news is that in 2016, Minnesota passed the test. We engaged a lot of different partners, including our partners at the state and local level, including looking for outside eyes and ears to sort of test our systems, and so we passed the test. We kept out the folks who were trying to get in.

From our vantage point in our office, we don't care who it is. We don't care if it is Russia or another foreign government or a non-governmental actor or the guy next door. We don't care what their politics are. We don't care what candidate they support or not. This isn't about Democrats or Republicans. This is about us as Americans.

We passed that test, which is great. But we know and we found out after the election that Minnesota was one of the 21 states that was targeted by elements acting at the behest of the Russian Government. That was the exact phrase that the Department of Homeland Security used in briefing us and letting us know about that threat.

We know we have to be vigilant, as we were in 2016, but now we have a lot more information. I think the good news here, the reason that the glass is half full, is that Minnesota—and I believe every other state—is in a far better position now going into this election than we were going into the last election, even though we passed the test in the last election.

As Senator Klobuchar alluded to, Minnesota is proudly old school. We have paper ballots, and that is the bedrock of our system in Minnesota. Very hard to hack paper, obviously. Although there are electronic components further on down the line, we feel that we have those well in hand in terms of state laws and some of the resources we need to attack those things.

Second, we think that we have benefited from the "critical infrastructure" designation from the Department of Homeland Security in terms of expertise, in terms of value added, in terms of a good partnership after a rocky start with those folks at Department of Homeland Security. That is good as well.

Third, DHS has put together, as you have heard, this Government Coordinating Council, which is a fancy term for people sharing information. Although that is good, I think it could be even better than it is right now.

Finally, we have the attention of not only you and your colleagues in Congress, but of the national and local media and of other elections administrators around the country, and that is very good.

In Minnesota—and I never miss an opportunity to brag about my state—we are number one in voter turnout in the country. Again, 74.7 percent of registered voters—or eligible voters, I should say, voted in the last election, and we are very proud of that. In some ways, that means the stakes are particularly high and that it hits particularly close to home for us in Minnesota.

We appreciate the Federal partnership that we have received so far, and I just want to say once again I want to thank everyone, including Senator Klobuchar and others, who were part of getting that $380 million for us, for elections administrators at the state. It is critical. It is crucial. We plan to use every penny of that $6.6 million over the next 5 years to good effect. It will go a long way.

However, I would respectfully request that those in Congress consider some ongoing way to provide some resources for us along those same lines. While we don't want to look a gift horse in the mouth and we are very grateful—and I know I am—for that money, this is expensive. The recommendations that we get from the Department of Homeland Security, while very helpful, they have a price tag, and that is not always accounted for in state budgets. I ask respectfully that you consider that as well.

Then on the policy side, I would be remiss if I didn't put in a word for the Secure Elections Act. I was part of the group of secretaries of state that Senator Lankford and Klobuchar invited to advise them a bit on the scope of the legislation, and I do think there is a legitimate Federal interest in making sure that we do have floors—not ceilings, not micromanagement—but some Federal interest in assuring that the states are talking with one another and that we are not just 50 silos doing our own thing in our own way.

Although we ultimately retain that authority to do so and we would never want that encroached upon by the Federal Government, I think there is an interest in making sure that there is some coordination, even if it is the states through the GCC or through other channels that decides what is best in terms of communication. If for no other reason than that, I think that is very important.

I thank you, Mr. Chair and Ranking Member Klobuchar, for your continuing efforts here and cooperation, and we look forward to an even more robust Federal partnership in the future.

Thank you.

[The prepared statement of Mr. Simon was submitted for the record.]

Chairman BLUNT. Thank you, Secretary Simon.

Mr. Masterson?

OPENING STATEMENT OF MATT MASTERSON, SENIOR CYBERSECURITY ADVISER, DEPARTMENT OF HOMELAND SECURITY

Mr. MASTERSON. Thank you, Chairman Blunt, Ranking Member Klobuchar, and members of the committee. Thank you for today's opportunity to testify regarding the Department of Homeland Security's ongoing efforts to assist state and local election officials, those who own and operate election systems, with improving the resilience of elections across America.

For over a decade, I have worked with state and local officials to advance the use of technology to better serve American voters. For the last 3 years, I served as a commissioner at the United States Election Assistance Commission, working to modernize standards used to test voting systems, provide best practices to help support election officials, and since 2016 respond to threats against our Nation's election systems.

Now I serve as a senior adviser at DHS focused on the work the Department is doing to support the thousands of election officials across this country. In this decade of work, I can tell you the absolute best part is working with the dedicated professionals like those seated at the table here with me that administer elections. In the face of real and sophisticated threats, these officials have responded by working with us, state and local resources, the private sector, and academia to mitigate risks and improve the resilience of the process.

Election security is a national security issue. Our mission at DHS is to ensure that the system owners have the necessary information and support to assess risks and protect, detect, and recover from those.

This support can come in many forms. Whether it is offering no-cost voluntary technical assistance or sharing general or specific threat information, DHS stands ready to help and offer tailored support based on state and local needs. Through these collective efforts, we have already seen significant progress. State and local officials and those private sector partners who support them are at the table working with us. We have created the Government Coordinating Council and private sector councils who collaboratively work to share information, share best practices, and develop strategies to reduce risk.

We have created the Election Infrastructure Information Sharing and Analysis Center, or EI-ISAC, with members from almost all states and hundreds of local jurisdictions. This is the fastest-growing sector in critical infrastructure.

We are sponsoring up to three election officials in each state for security clearances, which will allow officials to receive classified threat information if or when it is necessary. We have increased the availability of free technical assistance across this sector. DHS offers a variety of services, such as cybersecurity assessments, intrusion detection capabilities, information sharing and awareness, and incident response.

The progress being made is clear, as is evident by the testimony you have already heard today. Across the country, secretaries of state, state election directors, and local election officials are taking

the steps necessary to respond to this new and evolving threat environment.

Take, for example, the work of Secretary Lawson in Indiana. In addition to being an engaged and valued partner with us at DHS, she is taking advantage of our scanning and information-sharing services. Indiana has taken additional steps to improve their security, including increasing monitoring capabilities and tightening access and controls.

In addition, they are working to better secure their counties through implementation of two-factor authentication and improved post-election auditing. This story is true across the country.

We have seen firsthand the progress that is being made at the local level as well. Recently, Under Secretary Chris Krebs was in Orange County, California, where he was briefed on their comprehensive cybersecurity playbook. This plan includes improved cyber hygiene practices, more advanced network monitoring and intrusion detection, and the implementation of more robust, efficient post-election audits to ensure the accuracy of election results.

Combined, these best practices and security services greatly enhanced the resilience of Orange County's election system. By publicly communicating them, the county is working to give voters the information they need to have confidence that their votes will be counted accurately.

Elections are run by states and localities. Across the 50 states and 5 territories, there are over 10,000 jurisdictions that are responsible for elections. The systems, processes, and procedures used vary greatly. The local administration of elections empowers voters to engage directly with the process and those who run it.

Which brings me to my final point. For those voters who have questions or concerns regarding the security or integrity of the process, I implore you to get involved. Become a poll worker. Watch pre-election testing of the systems or post-election audits. Check your registration information before elections. Engage with your state and local election officials, and most importantly, go vote.

The best response to those who wish to undermine faith in our democracy is to participate and to vote. Moving forward, the Department will continue to coordinate and support state and local officials to ensure the security of our election infrastructure. Cyber actors can come from anywhere, internationally or within U.S. borders, and we are committed to ensuring a coordinated response from all levels of Government to help plan for and mitigate these risks.

Before I conclude, I want to take a moment to thank Congress for the legislative progress thus far in strengthening DHS's cybersecurity and critical infrastructure authorities. Specifically, we strongly support the final passage of legislation to create the Cybersecurity and Infrastructure Security Agency, or CISA, at DHS. This change reflects the important work we carry out every day on behalf of the American people.

I look forward to further outlining the work we are doing to enhance the security of elections, and I thank you and look forward to your questions.

Thank you.

[The prepared statement of Mr. Masterson was submitted for the record.]

Chairman BLUNT. Well, thank you, Mr. Masterson.

We will have a 5-minute round, and if everybody could stay pretty close to that and if people have other questions, we will have another 5-minute round. We do have a second panel, but we want to take full advantage of this panel.

Let me just ask first the three secretaries of state, this is yes or no, should the Federal Government be required to share information with jurisdictions that are being impacted by known threats?

Mr. ASHCROFT. Yes.

Mr. CONDOS. Yes.

Mr. SIMON. Yes.

Chairman BLUNT. For the three of you again, should that also—how would—should that include both the state, chief state election official as well as the specific jurisdiction? I think that is yes or no also.

Mr. ASHCROFT. I would say yes to that.

Mr. CONDOS. I agree.

Mr. SIMON. Yes.

Chairman BLUNT. Mr. Masterson, how would you determine—I know one of the things I believe you mentioned in your testimony was you would have to have some sense that someone was ready to receive that information in terms of cyber understanding or threat assessment. How would you really actually accomplish that with all the local election jurisdictions in the country, once you see they have a threat? Who do you think you should notify?

Mr. MASTERSON. The goal within the Department is to ensure broad notification across the sector, which is why we have worked to create the Elections Infrastructure Information Sharing and Analysis Center, so that there is an avenue by which threat information, risk information could be shared broadly. Then engaging with the Government Coordinating Council, creating those information-sharing protocols for the sector.

The number-one priority within the Coordinating Council has been to establish exactly the question you asked, Senator, which is how best to share information down to the states and then all the way down the locals to ensure that they have what they need and that it is done in a way that they can take it and it is actionable. They can use it to mitigate those threats and protect their systems.

Chairman BLUNT. In terms of broadly sharing, you mean you would also broadly share some information with people that could potentially face this threat whether they are currently facing the threat or not?

Mr. MASTERSON. Yes, Senator. That is correct. That is typical for how we share information within critical infrastructure is to try to boil down the nature of the threat and the information necessary for systems owners and operators to protect their systems across the sector.

Chairman BLUNT. Again, I am not quite sure I am clear on your view of what elected or appointed local official, what kind of qualification they would have to have, if any, besides having that job for you to share this information with them.

Mr. MASTERSON. In order—Senator, in order to receive the information from the EI-ISAC, they simply need to be local election administrator, state election official, or their support staff. The IT staff are eligible. In fact, we are working within the sector to craft this information sharing such that for executives like the secretaries of state at this table, they have the information they need to make good decisions from a policy and administrative standpoint, but that the IT officials, the technical folks also have the technical information they need to respond and protect the systems.

Chairman BLUNT. Is it possible you would be sharing with the technical official person something you wouldn't be willing to share with the elected official?

Mr. MASTERSON. No, Senator. All information is available to any of the election officials. It is just a question of who can best use that information to effectively protect the systems.

Chairman BLUNT. On the voter registration side, for the secretaries, do you have any sense of how many attempts there are to get into that system? Secretary Simon mentioned, appropriately I think, it doesn't really matter who is trying to get in, you don't want them to get in, whether it is a local political operative or a foreign government or somebody just seeing if they can get into that system and manipulate it in some way.

Is that something that often happens, people are testing the system to see if they can get in? Secretary Simon? We will go this way this time. You and then Secretary Condos.

Mr. SIMON. Mr. Chairman, yes. That is something that is known to happen quite often. Again, we and all the states here represented did pass that test, which is good. But there are people who are poking and prodding, and the analogy that I have come to use in talking with Homeland Security is imagine a car thief casing a parking lot, and maybe he goes there a day or two in a row. He takes out binoculars and he observes traffic patterns, and he tries to figure out is there a way in? That is what goes on and can go on quite frequently.

In the case of all the states represented here, for whatever reason, that car thief did not go into the parking lot. We would like to think it is because of the great cyber protections that we put up in the preceding years. But truth be told, we might never know the real reason, but we were able to keep them out. But there are people casing—there are a lot of people casing a lot of parking lots, and it is up to DHS to tell us who they are, what they are there for. So far, they have done that.

Belatedly with respect to the 2016 election—we didn't know until 10 months afterwards. But they are doing, I think, a better job every day of that.

Chairman BLUNT. Secretary Condos, is this a common thing that people are trying to test these systems?

Mr. CONDOS. Every day. We have—in talking to my IT manager, I can't speak specifically just for election management or the voter registration data base, but our entire operations, we probably receive several thousand scans per day.

Chairman BLUNT. Per day. Secretary Ashcroft?

Mr. ASHCROFT. I would say we average 100,000 scans on our systems a day. We cannot say which of those are targeted to elections. We have to treat them all as if they are treated toward elections because if they find one way in, they will go from there to elections. We treat them as they are all attacks on elections.

Chairman BLUNT. Yes, I am going to come back later, Mr. Masterson, to you on this topic and others, and how do we—how do you think we narrow down which of those should be reported and what should be followed up on? I am going to go now to Senator Klobuchar.

Senator KLOBUCHAR. Well, thank you, Senator Blunt.

We are just so pleased we are having this election hearing, and then I am going to defer to my colleague to ask questions first. I am glad they are here, and I will start with Senator Durbin. I wasn't kidding that I would defer to you with questions.

[Laughter.]

Senator KLOBUCHAR. I am just pleased they are here and that we are having this really important hearing in Rules. Why don't you go first, Senator Durbin, and then we will go in order of attendance. I will go last. Go ahead.

Senator DURBIN. Thanks. A few years ago, I was on the Senate Judiciary Committee, Chairman of the Constitution Subcommittee, and there was a lot of talk about voter fraud, voter IDs, reducing the time that you would be allowed to vote. I took the hearing on the road. We went to Ohio—Cleveland, Ohio. Then we went down to Florida. We called election officials just like yourselves, both parties, Republicans and Democrats, elected and appointed. I asked them the following question.

Your states just changed voter requirements to require the voters to prove with a voter ID, to limit the places where you can vote, to limit the time that you can vote. What has been the incidence of voter fraud in Ohio, in Florida that led you to conclude that you had to put these new burdens on voters? The answer was none. None.

For the record, I would like each of you election officials, if you would, please, pick—let us pick 10 years. Would you report to this committee, and you don't have to do it now, but if you would report to this committee, in the last 10 years, how many votes have been cast in your state and how many people have been convicted of voter fraud in either a state or Federal court in the same period of time?

I don't guess you will know this off the top of your head. I won't try to put you on the spot. But here is what I have concluded. The statement, Secretary Ashcroft, that you made is just—it has to be addressed for the record, and here is what you said.

Voter fraud is an exponentially greater threat than hacking. Exponentially greater. Let me tell you what happened in Illinois because we blew the whistle. We were one of the 21 states hacked by the Russians. They got into our voter file. Somebody left a little wormhole in there, and they got into our voter file.

They had the capacity, and thank goodness they didn't use it, to change just a digit on each of our addresses and make a chaotic situation at the polling place when people turned up to vote, resulting in hundreds of thousands of provisional ballots, and I don't

know how that would have ended. They didn't do it. Thank goodness they didn't, but the threat was there.

I could count on both hands the cases of voter fraud in the State of Illinois in the last several election cycles, and the convictions even fewer. When it comes to this hacking, it is exponentially greater threat to our voting system than voter fraud, exponentially. I am willing to say that.

I hope that we are ready. We put—thank you for the $380 million. It is good. We got $13 million in Illinois. I wish we would have gotten more. Three hundred eighty million will help. In 2002, HAVA produced 10 times that amount, $3.8 billion, to modernize our voting system.

I think the Russians are after us again. I hope I am wrong. I think other countries are after us again. If we spend all our time worrying about making it more difficult for honest American citizens to vote instead of worrying about what the Russians and others are going to do to invade our election system, shame on us.

I hope that we take this very seriously. I hope that all the states have a paper trail. Ours does, thank goodness. I hope every other state—I think five don't—will do just exactly that.

Secretary Simon, in your State of Minnesota, what are you going to use the Klobuchar funds for?

Mr. SIMON. Well, thank you, Senator Durbin.

We will use the Klobuchar funds. We have put in a request to use the first $1.5 million of our $6.6 million complement to redo our—what is called our SVRS, Statewide Voter Registration System. It goes by other names in other states. It is what it sounds like. It is the primary data base, the very one that, unfortunately, in Illinois suffered a breach and the very one that in most of the 21 states that I am aware of was at least the intended target at the end of the day.

Senator DURBIN. What they told me in Illinois, the State Board of Elections, I said what happened? How did the Russians get in there? They said we left a little opening that we didn't realize was there, and they got in that wormhole, and they were in our system.

They had the capacity. There is no evidence that they changed a single registration or a single vote. I certainly agree with the witnesses who have said that. From an Illinois perspective, that was true, too. But the potential was there for a dramatic change. Did you see the same potential in terms of your voter information and voting process?

Mr. SIMON. Well, Senator Durbin, without giving a roadmap to the bad guys——

Senator DURBIN. No, please don't.

Mr. SIMON I don't want to do that. But what I would say is that I think every system has some vulnerabilities. We, in 2016, did our very best to—and successfully—to make sure we took care of those vulnerabilities. We summoned people to find them. We asked for people to probe and poke and pry and find them so we could fix them, which we did.

As a result, I think we—and this is what many states have done, not just Minnesota. We managed to repulse or rebuff or turn away those who tried to get in, which is good, but I like to say this is a race without a finish line. There is no end zone where you get

to spike the football. There is no tape that you get to cross. You always have to stay one step ahead of the bad guys, and the bad guys get smarter every year. By the way, some of them are funded by foreign governments with virtually unlimited resources.

That race without a finish line is something that keeps a number of us awake at night, that takes effort, that takes focus, and it takes money. These things have price tags.

Senator DURBIN. Thanks. Thanks, Mr. Chairman.

Chairman BLUNT. Senator Cortez Masto?

Senator CORTEZ MASTO. Thank you. Thank you all for being here. I, too, want to thank you for this important hearing.

Let me just associate myself with Senator Durbin's comments initially. I was attorney general of Nevada from 2007 to 2014, and I can tell you I can count on one hand the type of voter fraud that we saw. Most importantly, not only did we see it, we caught it, and we prosecuted.

This idea that somehow there was widespread voter fraud occurring across this country that needs our immediate attention, which engages in voter suppression, is false. I so think that we need to correct the record and use accurate data.

But let me open this up to the panel as well. In Nevada, a majority of the counties are rural, and they obviously play a significant role in conducting elections in the state. The counties don't have the resources that more populous counties have, and they don't have resources like dedicated IT support. In your states, how have you addressed that unique challenge of election security faced by the rural communities, and what can we do to continue to help them and support them?

Mr. CONDOS. Thank you, Senator.

In Vermont, we don't have county government. We go directly from the state level to the towns, and in Vermont, the state is responsible for paying for the equipment. The state is responsible for ensuring that it is working, that it is maintained. We pay for the memory cards. We actually provide a lot of the resources to the towns. It is not a direct payment because we do the work.

That is how we approached it basically because of the way we are set up.

Mr. SIMON. Senator, in Minnesota, we have 87 counties. Only 9 of the 87 counties have full-time, year-round election staff. In most of the counties, which are rural or at least non-urban and metropolitan, those folks who run elections also wear many other hats. They do property taxes. They do drainage and ditch work. They do other things, and they don't have the luxury of focusing only on elections.

That is where I think, if I may, the Federal partnership comes in. It costs money to hire people, to have training, to put up the defenses. Hennepin County, which is Minneapolis, they might have the resources in terms of money and personnel and others to erect these kind of defenses. Other counties might not be so fortunate. That is where I think there is a Federal role to play, frankly, with money, with resources, to make sure that everyone in every state, regardless of where they live and what kind of community they live, can rest assured that the security in general and cybersecurity in particular is there and in place.

Senator CORTEZ MASTO. Right.

Senator CORTEZ MASTO. Was that the impetus behind your request for additional funds in your statement?

Mr. SIMON. Yes, Senator. It was in part. I mean, I think making sure we have an even playing field no matter where a voter lives in Minnesota is very important.

Senator CORTEZ MASTO. Okay, thank you. Anyone else?

Mr. ASHCROFT. In Missouri, we have really 116 election authorities. We have some counties that are split up. We have counties with roughly 2,000 registered voters. They do not have the ability and the wherewithal on their own for IT staff. Our office works with them.

We have had meetings with our directors of elections, going around the state to reach out to them on new cybersecurity initiatives. We are holding a national cybersecurity conference, both for secretaries of state, for national officials, and local election officials on September 10th and 11th. We are putting all of our effort—well, not all of it, but most of our effort into making sure that they have actionable things they can do and the resources to do it.

I would add one other thing. When we passed voter ID in Missouri, we actually increased accessibility to the ballot. We actually have individualized individuals that would have been turned away under the old law that were allowed to vote on our new law. I understand Illinois doesn't work as well as Missouri, but in Missouri, we can secure our ballots and make sure that every registered voter can participate and their voice is heard.

Thank you.

Senator CORTEZ MASTO. Thank you. I appreciate those comments.

I also think we can also do automatic voter registration and still secure our elections and make sure everybody has access to vote.

Let me also say this, Mr. Masterson. I think you need to know this. I worked very closely with the election officials. In fact, I think it is true. Everybody should volunteer. I volunteered in Clark County on election site when I was an assistant county manager.

But know this. I want to convey to you that the election officials in Nevada have told my office that DHS has been great to work with. Extremely helpful. Generous with your services and knowledge. Thank you for that. I really appreciate it.

One of the things they told me, however, and I am curious if you are hearing this and if this is true, and it is not a negative thing. It is that there is too much information, that they don't have the bandwidth to process the daily DHS updates and have difficulty figuring out what pieces of information are relevant for them and establishing priorities among the information overload.

Are you hearing the same thing?

Mr. MASTERSON. Thank you, Senator, for the question, and I think this may go to Chairman Blunt's question as well.

We have heard some of that, and part of what we are trying to tackle—you know, as you establish a new sector, this is a new flow of information to election officials—is finding that balance about what is the right amount of information, tailoring it in a way that prioritizes what they really need to know. But then ensuring that

the technical folks or IT folks that perhaps need a little more detail and more constant updates have that as well.

I think we are finding that balance as we work with the Government Coordinating Council and some of the folks at the table to create that tailored information sharing. We will get better as we build that relationship and share that information. But, yes, that is something we have heard and we are working to get better at.

Senator CORTEZ MASTO. Thank you.

Chairman BLUNT. Thank you, Senator.

Senator CORTEZ MASTO. Thank you.

Chairman BLUNT. Senator Udall?

Senator UDALL. Thank you, Chairman Blunt.

Let me just, before I ask a couple of questions, we had a previous Secretary of State by the name of Dianna Duran, who made these just widespread accusations about voter fraud, and our state very conscientiously went through thousands and thousands that have been reported. After review, it came down to several, I mean just a handful of unintentional minor errors. No one was ever prosecuted. There was never any real fraud that was found.

I think we need to be very, very careful. I mean, she got wonderful headlines, you know? For weeks, there was all this activity of, "Oh, there is fraud. There is fraud." Then, when it finally trickled out and everybody reviewed it, there was nothing there.

I want to focus again, Secretary Ashcroft, on the quote that Senator Durbin asked. The evidence indicates that voter fraud is an exponentially greater threat than hacking of election equipment. What studies or evidence, preferably independent academic studies, back up that claim?

Mr. ASHCROFT. Well, the Senator's actually own words back it up because the Senator said that the allegations showed that there were no votes changed, no registrations changed by hacking. Yet I gave concrete evidence of an election being changed by vote fraud.

As far as I am concerned, if elections are changed by fraud, be that individuals in Missouri, be that individuals overseas, or by ineptitude, anything that stops the voice of the voting public from being heard and then making a decision, that is a problem. What I said in my remarks is still true. We should take a comprehensive approach to make sure that no votes are changed by fraud, malfeasance, criminal actions, or ineptitude. We should make sure that every voter knows their vote will count.

Senator UDALL. Well, you didn't answer my question. My question was about your statement here, "exponentially greater threat." What proof do you have?

I mean, we are all against fraud. Nobody wants fraudulent voting. But what proof, independent studies to back up your claim that it is exponentially greater?

Mr. ASHCROFT. I will say it as simply as possible. Your colleague admitted that no votes were changed, no voter registrations were changed by the alleged hacking. I gave you a concrete example that was proven in a court of law as individuals pled guilty of changing an election.

No instances of votes being changed. An instance of an entire election being changed. That is exactly what I am speaking to. I don't know how I can make it more clearer, sir.

Senator UDALL. The—and this is for all the secretaries here, and Mr. Masterson, if you have anything to add, I would be happy to hear it. Secretary Lawson's written testimony stated that only 59 percent of states have drawn down their HAVA funds. We know that every state's election infrastructure is vulnerable in some way, shape, or form, and we also have heard over the years that elections are underfunded.

Let me ask each of the secretaries, have you drawn down your HAVA funds, and if not, what is preventing you from doing so? It is a pretty simple answer. I don't need a big lecture on that one.

Mr. ASHCROFT. Missouri was the first state to draw down their HAVA funds.

Senator UDALL. You have drawn them all down. Okay. You have drawn them all down. Go ahead.

Mr. CONDOS. Vermont has already drawn down their $3 million.

Senator UDALL. Yes, Mr. Simon?

Mr. SIMON. Thank you, Senator. We have drawn down our HAVA funds.

Senator UDALL. Do you want more? Could you use more?

Mr. ASHCROFT. If you send it, we will use it, sir.

Senator UDALL. Yes. Same?

Mr. CONDOS. Yes. Actually, I think what we really need is ongoing—if you want to call it maintenance. Cybersecurity is an evolving science, and it is an evolving practice. We have continuous needs going forward.

Senator UDALL. Same, Mr. Simon?

Mr. SIMON. I would echo the sentiment, yes.

Senator UDALL. Thank you. In your conversations with other secretaries of state, do you hear reasons why other states aren't drawing down these funds?

Mr. CONDOS. Senator, I would say that some of the states have to deal with legislative action that needs to be taken in order to accept Federal grants. Some of the states may be required to do that first. Or it could be from their administration. The Governor's office may have to approve it before it can be drawn down.

I think there are other states who are probably trying to plan out what they are going to be doing with the money just before they get the money.

Senator UDALL. Yes, Mr. Ashcroft, did you have a comment on that?

Mr. ASHCROFT. I would say the EAC did a phenomenal job getting it out quickly. If it had been a week later, we would have run into problems with our legislature.

Mr. SIMON. Senator, I just want to make a distinction between the initial HAVA money in 2003. That, we have drawn down. The latest chunk, what we have been calling affectionately "the Klobuchar money," unfortunately, because of, frankly, a political fight in our legislature at the end of the session, we weren't able to get access to that $6.6 million now, this year.

That was a totally avoidable outcome and an unfortunate one. We think we will be okay, but the sooner we can get that money, the better.

Senator UDALL. Yes. Thank you for the courtesy, letting me go over a little bit, Chairman Blunt.

Chairman BLUNT. Thank you. Senator Klobuchar?

Senator KLOBUCHAR. Thank you very much.

Just to clarify, Secretary Simon, you will be able to access that money in the future, and the legislature and the Governor appears to want our Secretary of State's office to get that funding. Is that correct?

Mr. SIMON. That is correct.

Senator KLOBUCHAR. Okay. It was just part of a larger fight over something that, as you described it, was unfortunate. It wasn't about the money.

You mentioned, Secretary Simon, that the bill strikes a right balance of the Federal Government support for states. This is the Secure Elections Act. Can you expand on this?

Mr. SIMON. Right. Well, I, along with my colleagues, I think regardless of party, will always emphasize the primacy of the role of states in administering elections. I think there is, I dare say, unanimity on that score among secretaries of state.

But what I like about the balance that the Secure Elections Act is striking, and I know it is a work in progress, is this realization that floors, not ceilings are okay, that even if it is just a question of a Federal interest in making sure something is done, regardless of how the states choose to do it, is important. I highlighted in my testimony here just the communications process.

The GCC, the Government Coordinating Council, is already coming up with communications protocols, and my understanding of the latest version of the Secure Elections Act is there is an acknowledgment there, that that communications can come in many different forms including, and not limited to, what the GCC comes up with. But the important thing is that there is communications, by the way, not just up and down, but up, down, and sideways. Local Governments, State Governments, Federal Government, maybe some nongovernment actors in some situations.

I think that alone is a cause for the Federal Government to assert some interest in making sure that this communication is going on. An election attack in Minnesota can perhaps be linked to or have very real effects on an election attack in Vermont or Missouri or anywhere else, and so I think that communications is important.

I highlighted that particular aspect, but I think a recognition of the primacy of the state role, coupled with a very real and genuine Federal interest in making sure things get done. States can choose how those things get done. I think that strikes the right balance.

Senator KLOBUCHAR. Okay. Secretary Condos, you mentioned that the Election Assistance Commission has done a great job of disbursing the HAVA funding, appropriating earlier this year this money we are discussing. Much of our focus today has been on DHS, but could you comment on the role that EAC has played in improving communications around the cybersecurity issue.

Mr. CONDOS. Certainly. They have been a very valued partner with us. They provide information. Obviously, we have to submit an approved plan or a plan to them how we are going to spend the money.

I think, you know, I may differ from some of my colleagues, but I think that the EAC plays an important role in our elections process across this country and sorely needs to have the resources it

needs to operate and also really badly needs to have Congress appoint a full quorum, at least a quorum so that they can—their board, or the commission can actually operate.

Senator KLOBUCHAR. You mentioned your support of post-election audits earlier. Can you expand on the importance of conducting audits and how it relates to voter confidence?

Mr. CONDOS. I think that that is extremely important for all the—for the integrity of our elections. We in Vermont do use paper ballots, and we do a post-election audit within 30 days. When we do it, we actually do approximately 5 percent of our towns, and we do 100 percent of the ballots from that town, 100 percent of the races on that ballot.

We do a complete audit of that election. We feel that the confidence level that we have with it is as close to 100 percent as you can be. It is a post-election audit is something that I believe should be something that is included in the Secure Elections Act as it is.

Senator KLOBUCHAR. Secretary Simon, same question, but about paper ballots and how you see them as an advantage.

Mr. SIMON. It is a huge advantage, especially post 2016. I mean, the fact that Minnesota is proudly old school has served us well, and we see now many states that are—who were once perhaps sold on this vision of the paperless future are now understanding that, no, paper is good after all and are going in the direction of most of the states in having a paper ballot.

It is very hard to hack paper, and although in Minnesota, that paper is fed into a machine, under state law, that cannot, must not, and shall not be connected to the Internet. That is a central part of our system.

Senator KLOBUCHAR. Then you have been able to get results fairly quickly with this system?

Mr. SIMON. That is right. Yes. It also benefits those following the results on election night because the results can be reported very quickly, and the counties and the local governments are outstanding partners in making sure we get that information out.

Senator KLOBUCHAR. Okay. I can turn it to you and then maybe ask a few questions——

Chairman BLUNT. No, go ahead. We have some time.

Senator KLOBUCHAR. Okay. I want to focus on some of the things that have come out here. First of all, I am not going to go on about voter fraud, but I will note the decision that came out just yesterday in Kansas, where a Kansas judge struck down Kansas' voting registration law that they had introduced, that Secretary Kobach actually had introduced that was very restrictive.

He had made this case that there were—it was the tip of the iceberg, the people that he had found who had somehow fraudulently voted. The judge here looked at all the evidence and found that it was a very small number and said that there was, in fact, no iceberg—this is their words—only an icicle, largely created by confusion and administrative error.

This was a very thorough review of this. This is based on my own experience as the county attorney in Minnesota's biggest county, where we had to review cases that were referred to us from the Secretary of State, and I had a full-time investigator. This is right on the front line looking at these. I would—I would echo these re-

marks because I remember specific cases, the handful of cases people referred to.

The couple whose—the voting line went right, through the school board, through their house, and they had decided that meant that each of them could vote in both elections, and then they asked me where they were supposed to vote, and we did research and said it was where they sleep. Then the wife called back and said, well, what if we slept in separate beds on two sides of the line?

Okay. I don't—I mean, this is serious stuff, but the kind of cases I saw, and we did prosecute a few. A guy that said a Republican wouldn't have a say in Minneapolis. So he decided to vote twice. Told that to our investigator.

We had—but those were so rare. Overall, we found that most of these cases were a dad and a son with the same last name and the same first name, and it was confusing. When we looked into it, we found out they had a total legal right to vote.

I do want to remember this decision, which really encapsulates what we have seen in these studies all across the country and that our effort should be much more on trying to get people to vote, which secretary of states are in such a unique position to do, to encourage them to vote, to get the numbers up. For us, it always works to say we don't want Iowa to beat us in voter turnout, or we don't want Wisconsin to beat us. But that is what we should be doing and not—and be honest about what is going on here with these numbers.

Then the other thing we have to be honest about is not that the votes were changed in the last election, but they tried, and they tried hard, and they got into the Illinois data bank, and those kinds of things. They tried in 21 states.

When our own intelligence people under President Trump are telling us that Russia is emboldened, are telling us that we are at risk, I think we have to pay attention to it. I appreciate that is why we are having this hearing.

My question of the panel, just a yes or no, the 2018 primaries already happening across the country, general election 139 days away. You are on the front lines. Confirm, yes or no, do you agree elections are a potential target and, therefore, you see this as a priority? That is my question.

Secretary——

Mr. ASHCROFT. Primary elections are a very big priority to us, and we have already started implementing things.

Senator KLOBUCHAR. Good. But do you see election security as a priority?

Mr. ASHCROFT. I think that is a very important topic, and that is why we have been working for quite a while.

Senator KLOBUCHAR. Okay. Sure.

Mr. CONDOS. Simply put, yes.

Senator KLOBUCHAR. Okay.

Mr. SIMON. Yes.

Senator KLOBUCHAR. Okay.

Mr. MASTERSON. Yes.

Senator KLOBUCHAR. Okay. Secretary Ashcroft, from your testimony, it sounded like you believe that information sharing from

the Government to the states is important and that it should be improved. Do you want to—you can elaborate on that.

Mr. ASHCROFT. Yes. There have been serious problems with prior individuals in DHS. We had a NASS meeting last year where DHS reported that they had told states about instances, but they couldn't tell us who they had told. They hadn't told chief election officials. They might have told the chief technology official. They might have told a local election official.

We have had problems with things being classified far above what they should be classified. They couldn't tell that to election authorities, and we couldn't respond.

Senator KLOBUCHAR. Yes, seen that. Very good.

Mr. ASHCROFT. Sorry.

Senator KLOBUCHAR. No, no. It is just very—I mean, I said I have seen that, and that is well put and must be incredibly frustrating when you are trying to do your job.

We discussed already, Secretary Condos, the post-election audit process. We talked about paper ballots and how important this money is.

Mr. Masterson, in a recent article, you wrote about some of the great work election officials are doing around the country. Do you believe that state and local election officials can benefit from this sharing that we talked about? This is not just the immediate information about the threat that we need to have happen, but also best practices.

Mr. MASTERSON. Absolutely, yes.

Senator KLOBUCHAR. Okay, very good. Well, I went through all those because those are the elements of our Secure Elections Act. Very tricky, huh? We are just hoping that we can get this through, and I know Senator Lankford is working very hard to do that.

But thank you all.

Chairman BLUNT. Thank you, Senator Klobuchar.

Let me start back to where I was a minute ago. In the Secure Elections Act, which is a work in progress apparently that we will take up at some point, one of the requirements there is that if an election agency has reason to believe that an election cyber incident has occurred with respect to the election system, they are to notify the Department. That would be the Department of Homeland Security. That is earlier defined as "any incident, any incident involving an election system."

Clearly, from the numbers that have been shared here, that would be an unreasonable thing to do. I think maybe, Mr. Masterson, maybe in the interest of time, we may just have to come back to you and your—the GCC and say how do we write that in a way that it makes sense? You obviously don't need 1,000 a day or 100,000 a day notices that somebody is trying to get into our system.

We need to figure that out. Do you want to comment on that?

Mr. MASTERSON. Mr. Chairman, I would agree completely. I think finding that balance is something we have been discussing in the GCC. None of these folks or the locals need notice that their Microsoft patches are out of date, right? They are aware and working on that.

What is the balance on notification with regard to threats, vulnerabilities, and incidents and finding that balance? So happy to report back and work with that.

Chairman BLUNT. Exactly. On the audit trail, do all three of your states require an audit trail? Do you require a paper ballot trail, yes or no?

Mr. ASHCROFT. Yes, we do.

Mr. CONDOS. Yes, we do.

Mr. SIMON. Yes.

Chairman BLUNT. Same, the same response, yes or no, should the Federal Government make an audit trail, a paper audit trail a requirement to have Federal assistance?

Mr. ASHCROFT. I don't think so.

Mr. CONDOS. I do think so.

Mr. SIMON. I think there is a Federal interest in making sure that there is some audit, some audit process.

Chairman BLUNT. Well, now what I am asking about is should there be a way to re-create the actual election itself? I don't know quite how to do that without paper, even if you had a machine that was not accessible to the Web.

Mr. ASHCROFT. I believe states are moving to do that without Federal legislation. That is why I don't think Federal legislation needs to be done on that.

Chairman BLUNT. But in all three of these cases, you have that. On the audit requirement, how specific do you think that needs to be? If we had a—in this bill, there is, I think, a specific—you have 5 percent. Should that be left up to you, or should we tell you whether 5 percent is enough or not, depending on how close the election was?

Mr. CONDOS. That is a great question, Senator, and I think that really there should be some flexibility in the type of audit as well. I mean, we hear a lot these days about risk-limited audits. Risk-limited audits are a great way of doing it if you have the systems in place that allow you to do it, and right now, there is only a handful of states that could actually do that.

The system that we use, as I said, we are actually talking internally about increasing the 5 percent to maybe 8 percent or even 10 percent of our towns post election. We feel very confident that it is actually even better than a risk-limited audit because it actually looks at 100 percent of the ballots that are cast in a town and 100 percent of the races. So you are auditing the entire ballot bag essentially at that time.

Chairman BLUNT. Any comments from the two of you on that?

Mr. ASHCROFT. When I was teaching, I taught statistics. I think that the language should just give probability intervals or confidence intervals as opposed to a specific percentage. For a very close race, you need to look at more. If it is an 80–20 race, you don't need to look at as many ballots for people to have confidence.

Chairman BLUNT. Secretary Simon?

Mr. SIMON. Senator, I would say the more flexibility, the better. There are states, without throwing any under the bus here, that are not represented here today. They don't have really any or any meaningful sort of audit, and it strikes me that there is a Federal interest in making sure that there is some audit process.

Chairman BLUNT. When you do an audit, do you count the ballots the same way they were counted on election day?

Mr. SIMON. Yes.

Chairman BLUNT. How about you?

Mr. CONDOS. We use a completely different system, completely different tabulators.

Chairman BLUNT. But you don't hand count them or anything? You still count them——

Mr. CONDOS. No. In fact, in our experience, the hand counting has actually proved to be the most error.

Chairman BLUNT. Secretary Ashcroft?

Mr. ASHCROFT. We don't hand count everything, although there are times when we do, and we are working with the local election authorities on those rules.

Chairman BLUNT. Would you give a direction in that post-election audit to election authorities locally, and they do the recount, or you do the recount?

Mr. ASHCROFT. The local election authorities do the recount.

Chairman BLUNT. How about with you?

Mr. CONDOS. We do the—we do the audit entirely.

Chairman BLUNT. The ballots come to you in the State capitol, and you do the audit, or you go to where the ballots are?

Mr. CONDOS. We do a public audit. We use the auditorium in the Governor's building, and we have the ballots delivered to us by the local boards of civil authority from each of the towns that have been randomly selected. They deliver those ballots to us. We do our work, seal those ballots back up in the bag, and get them delivered back to the towns.

Chairman BLUNT. How do you do it, Secretary Simon?

Mr. SIMON. Senator, that is done at the local level, not by our office. But we then followup with a second step some weeks later and do what is called a post-election review of that audit.

Chairman BLUNT. Right. All right. I think there will be more questions for the record, and certainly, Secretary Ashcroft and I are really glad that all these states have these great good government traditions. Our tradition is not quite that great. If you looked at the 2000 Governor's race in Missouri, I think there is a post-election investigation that finds out lots of people voted who shouldn't have, including a dog.

We don't know exactly how the dog voted, but the dog was the person—was the registered voter, and the ballot was cast. So, you know, we are not—just to get this discussion where I think it should be, the Federal Government is not about to do things that encourage voter fraud, and the discussion that voter fraud doesn't happen is not really before the committee today, but I look forward to your reports back of what kind of voter fraud you have had.

I think, Secretary Ashcroft, within the last year, we had one election that was set aside by a court, two elections, according to Secretary Ashcroft, set aside by a court, and then they had to have the election again. Was that absentee voter fraud, or was that voter fraud at the voting place?

Mr. ASHCROFT. It had to do with the absentee ballots. There were serious allegations of absentee voter fraud. They didn't have to

prove the voter fraud. There was enough smoke that the court said redo it.

Chairman BLUNT. We even have courts in our state that say you have to have the election over again. I guess we just have a burden that Illinois doesn't have or other states that don't think this is ever a problem. It is a problem. It happens not to be the problem we are dealing with in this bill, in this hearing, or right now.

Thank all of you for coming. We have got a vote coming up before too long, so if our next panel will come up, we will have some questions for our local election officials, one of which is from the Illinois jurisdiction that somebody actually got into, as opposed to the 21 jurisdictions that people tried to get into.

[Pause.]

Chairman BLUNT. All right. Our two witnesses here are Noah Praetz, who is the Director of Elections working under Cook County Clerk David Orr. I am not quite sure, but we are going to find out if it was your jurisdiction or another one that somebody actually got into, Mr. Praetz.

And Shane Schoeller from Springfield, Missouri, where I live and vote and has a job I once had. Let us start with Mr. Praetz and then Mr. Schoeller, and we will have a few questions for both of you.

OPENING STATEMENT OF NOAH PRAETZ, DIRECTOR OF ELECTIONS, COOK COUNTY, ILLINOIS

Mr. PRAETZ. Thank you, Chairman Blunt, Ranking Member Klobuchar.

My name is Noah Praetz. I am the Director of Elections in Cook County, Illinois, and it is a real honor to be here.

As election administrators, when we certify results, we help bestow not just power, but legitimacy. Legitimacy that comes from the essential American belief that our elections reflect a trusted and true accounting of voter choices. That legitimacy must be secured.

Election officials have been working and securing votes and voter records for a very long time. When I started in the business prior to 2000, we served mostly as logistics managers, like wedding planners, making sure the right lists of people came together in the right place with the right stuff. After *Bush v. Gore*, though, and the Help America Vote Act, a new era of rules and voter technology was heralded in, and we became legal compliance and IT managers.

But the 2016 election and all advice shared since show that sophisticated attacks are to be expected, and therefore, we must become cybersecurity managers. Spurred by this need to defend against foreign enemies, officials have been working successfully to find a good balance of Federal involvement in elections without trampling on the authority that states zealously guard. Good progress is being made.

State officials who protect statewide voter registration lists everywhere and more systems in some states and who are often the spokespeople defending our institution deserve great credit, particularly their lead blocking up to the 2016 election. However, and at the risk of being overly broad, I must underscore today that local

election officials are the ones who control, secure, and run elections.

We locals, 108 in Illinois and over 8,000 nationally, are on the front lines of this new battlefield. We deploy a variety of network-connected digital services such as voter registration systems, informational websites, unofficial election results displays, electronic poll books, election day command centers, not to mention the less-connected vote counting systems. Each of these is a target for our adversaries.

Most of us are simply county officers, and we are facing down powerful, shadowy adversaries like Andy of Mayberry sent to repel an invading army. We need advice, support, and resources. First, for modern, defendable technology and routine hand-counted audits, which can give additional confidence that digital results are accurate. Second, and more critically today, we have a pressing need for top-notch security personnel with the skills to navigate the current cyber minefield.

In Cook County, we have studied this, undertaken significant efforts at securing our infrastructure, and helping raise awareness broadly through the ecosystem. We conclude that to decrease the likelihood of successful attack, each election official must have access to an election security officer. Most election officials don't have that today.

We suggest this be handled by a brigade of digital defenders or, as Homeland Security's Coordinating Council calls them, "cyber navigators." These navigators should adopt a mantra of "defend, detect, recover." They can help us improve defenses following the specific recommendations of the Center for Internet Security or the Defending Digital Democracy program at Harvard. They will also help us mature our breach detection techniques, and they will help mature our recovery plans for when attackers penetrate the first and second line.

To accomplish this, the navigators will secure free support on offer currently from Homeland Security, state governments, and companies like Google and Cloudflare. They will work with state and county IT staff and with vendors who support locals in much of their support.

Finally, they will help build a culture of security that can adapt to evolving threats. Incidentally, Illinois lawmakers recently required that half of the HAVA funds you just released be spent on a navigator program, and our state election officials are acting aggressively to create one.

Voters across the country should feel broadly confident that we have resilient systems, and election officials are taking this problem very seriously. But voters should also understand that without continued investment in people and products, the possibility of a successful attack increases.

Some losing candidates are already apt to call their defeats into doubt. A new digital breach, no matter how far removed from the vote counting system, could turn sore losers to cynicism, disbelief, even revolt. That is the reaction the enemies of the United States want.

The bottom line is we cannot eliminate every chance of breach, but we can make sure that successful attacks are rare, and we can

provide assurances that we are prepared to recover quickly when they do happen. We can do this with support at the local level.

But democracy is not perfect. As Churchill noted, it is the worst form of government except for all the others. We need to protect it, and we will regret it if our democracy is damaged because we looked away and failed to support it at this critical moment.

Thank you, and I look forward to any questions.

[The prepared statement of Mr. Praetz was submitted for the record.]

Chairman BLUNT. Thank you, Mr. Praetz.

Mr. Schoeller?

OPENING STATEMENT OF SHANE SCHOELLER, CLERK, GREENE COUNTY, MISSOURI

Mr. SCHOELLER. Good morning, Mr. Chairman, Ranking Member Klobuchar, 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 the County Clerk in Greene County, Missouri.

The county clerk in each county of our state is responsible for several administrative duties for the county. These duties 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. Election administration is clearly the most visible duty of all that I just mentioned.

It is a duty that my fellow county clerks and election directors across the state take seriously as we work tirelessly to ensure the correct ballot is 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, but not unique in being responsible for several other administrative duties. This effort in large part is decentralized state by state and county by county, which is an advantage in protecting against a broad-based systemic cyberattack on our elections.

The advantage of being decentralized for local election officials is also a challenge as it relates to cybersecurity threats 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 office, and the coordinated efforts of the Department of Homeland Security and the Election Assistance Commission to be their firewall for protection against incoming cybersecurity threats.

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 the DHS and the National Association of Secretaries of State 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 that would change the

"Technical Guidelines Development Committee" to the "Technical Advisory Board" and, because of that, include cybersecurity experts as part of it.

I believe changes like this are needed to build on the current information sharing that was not in place prior to the 2016 election to continue improving how cybersecurity information is shared to local election officials in a common sense and productive way, to help mitigate possible cyberattacks in future elections.

I do want to address one area of concern in the Secure Elections Act, and that is on page 23, lines 3, 4, and 5. 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," as I believe the opportunity for fraud in an electronic ballot casting system that does not have a paper trail is too great.

To this point, part of the post-audit requirements in our state's regulatory code requires a manual count of the voted paper ballots based on a random drawing by a bipartisan team not less than 5 percent of the 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 during the post audit was critical to helping earn confidence that the certified election results in the 2016 general election were accurate.

An area of concern that has received less focus, but cannot be underestimated, is the possibility of an attempted cyberattack 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, and it is a convenience voters really appreciate as they see their wait times reduced.

This convenience, though, can quickly evaporate and become the source of real issues on election day if voters who have not voted are informed on election day that they already have 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.

As we think through these issues, it is evident that a majority of our local election officials, who balance so many administrative duties for their county and often have no resources available to monitor and prevent incoming cyberattacks, need outside help from the DHS and their secretary of state to help them withstand future cyber threats through their voter registration data and the tabulated election results on election night.

It is for these reasons that I recommend that the 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 the 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.

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.

[The prepared statement of Mr. Schoeller was submitted for the record.]

Chairman BLUNT. Thank you, Mr. Schoeller.

How many registered voters approximately do you have in Greene County?

Mr. SCHOELLER. Just a little over 189,000.

Chairman BLUNT. How about you in Cook County?

Mr. PRAETZ. One-point-five million.

Chairman BLUNT. Was it your system that was penetrated by some—by a hacker we believe to have been a Russian hacker?

Mr. PRAETZ. It was a statewide system. Illinois is a little bit different. We are——

Chairman BLUNT. The State Director of Elections would have been the person that we would have seen on 60 Minutes not too long ago talking about this?

Mr. PRAETZ. Yes, sir. That was him. Yes.

Chairman BLUNT. It was the statewide Illinois system?

Mr. PRAETZ. That is correct.

Chairman BLUNT. Is it your view that more problems are likely to be created on election day by getting into the registration system than the likelihood of getting into the counting system?

Mr. PRAETZ. Sure. I mean, we have got a broad threat surface area. We rely on a number of different systems. The network connectivity of voter registration systems is certainly much greater than voting systems and, therefore, more—an easier target for adversaries.

Chairman BLUNT. Mr. Schoeller?

Mr. SCHOELLER. I would concur, and certainly that is an issue that happened in Durham County, North Carolina, in 2016, very small scale. But if you would increase that scale, you could easily see the issues it would create on the day of an election.

Chairman BLUNT. The option of provisional voting, as Senator Durbin suggested earlier, it would quickly sort of overwhelm the system if you had all kinds of people trying to cast their ballot?

Mr. SCHOELLER. Correct. We are looking at a back-up system in case that would occur for our county. But clearly, even that is going to be fairly technical and hard to accomplish. But we are looking at that, should that occur.

Mr. PRAETZ. If I might point out, please, that in Illinois, we have got election day registration, which, in and of itself, is a highly resilient policy decision that our lawmakers made, particularly in the event of an issue with the voter registration data base. Clearly, lines become a problem. We have been modeling—our election day registration now is about 10 seconds longer than our normal check-in.

There are ways—there are ways to do it, but it is a policy decision that not only helps the voters, but it makes the security of the whole system much more resilient.

Chairman BLUNT. I assume if you could register in 10 seconds, you could also do what you need to to cast a provisional ballot pretty quickly then?

Mr. PRAETZ. Sure. That is true.

Chairman BLUNT. If that same system was designed to accommodate that?

Mr. PRAETZ. Yes, sir. Absolutely. It is 10 seconds marginal increase.

Chairman BLUNT. Yes.

Mr. PRAETZ. I would love to be able to get voters through in 10 seconds, but that is not the case.

Chairman BLUNT. Mr. Schoeller?

Mr. SCHOELLER. Right now, our provisional ballot process would not allow for that to happen quickly because of the process in filling out the envelope, all the details that go along with that. We are certainly—Illinois may be ahead of us in that particular regard.

Chairman BLUNT. Do you have a way, Mr. Schoeller, to monitor how many people might be trying to access your system from outside the system?

Mr. SCHOELLER. That would be through our information systems team, and they keep that information pretty close to the vest, but we are fortunate in Greene County, we have that type of help available. But clearly, in our smaller counties, I was visiting with one of my fellow county clerks before today, and they said we are not prepared, if something of this scale would occur, to be able to defend themselves.

Chairman BLUNT. Now I was in a location in St. Louis a couple of weeks ago where they have—really they are the principal provider of the iPad voting day system.

Mr. SCHOELLER. Yes.

Chairman BLUNT. They were just transitioning 51 counties in Minnesota to that system. They just got the entire country of Canada as a client. One of the things they were doing while I was there, they had three summer interns and two other people who just all the time tried to get into the systems that they are responsible for.

You know, this is somebody who spends all day every day trying to secure a system by trying to penetrate a system. If they find those spots, so you have people doing that.

Mr. PRAETZ. Sure. I mean, the red team attacks are very valuable sort of efforts to ensure that your defenses are holding up as you would expect. Homeland Security has offered that to all the states and locals. We just had a risk and vulnerability assessment through them, and it is quite interesting what the good guys are capable of as well.

Chairman BLUNT. But the good guys have to be—you know, our whole cyber structure is the good guys have to be successful all the time.

Mr. PRAETZ. Every single time.

Chairman BLUNT. The bad guys only have to be successful once to do—to do great damage. Before I turn to Senator Klobuchar, Mr. Schoeller, you would like to see a paper ballot as part of a national requirement?

Mr. SCHOELLER. I would in terms of as you think about the measurement that is used in all the different things, but particularly when you are visiting the voters. A voter wants to see something tangible, and I think the tangibility of paper is going to give them much greater confidence. I think when it comes to Federal elections, not just for President, but for the balance of Congress and the House and the Senate, that being able to give them that assurance that, yes, we can always go back and look at a paper trail versus something that is on a screen that is based inside a system that we have to trust. I think voters are going to appreciate that type of assurance.

Certainly, when I visit voters back home, I rarely have a disagreement. Matter of fact, I can't think of one time a voter has disagreed with me in that regard, regardless of party.

Chairman BLUNT. When you do an audit of the post-election audit, you count those by hand or with counting equipment?

Mr. SCHOELLER. We—at no less than 5 percent of the voting precincts on the day of the election, we do—and they are bipartisan teams. They are recounted by hand. One of the things that I think is important is that even if you do a post audit with a machine, how would you know if something has been compromised if you can't at least compare the results of the paper ballot, and I think that is the assurance it gives.

Clearly, the machine, when you have an accurate election, does do a better job of counting the ballots. I am talking about in the case where, clearly, fraud has occurred. Then the paper ballot is going to be the evidence you need in terms of if your system inside that machine is compromised.

Chairman BLUNT. Thank you.

Senator Klobuchar?

Senator KLOBUCHAR. Thank you very much, Mr. Chairman.

I think for a while people were talking about, well, why doesn't everyone just vote from home, which is great when you can mail in a ballot. We know that. But vote from home just from your computer, and that would mean no paper records of anything. Could you comment about that?

Mr. PRAETZ. I think that is 100 percent inappropriate for civil elections.

Mr. SCHOELLER. I find it ironic because this is my first term. When I ran for this office in 2014, that was actually a common theme that I heard.

Senator KLOBUCHAR. Right. I was hearing it, and I was—I kept thinking about our state with, I am not going to keep dwelling on it, with that high voter turnout. But you know, that involved the paper ballot——

Mr. SCHOELLER. Right. That was incredible integrity.

Senator KLOBUCHAR. Incredible integrity. But it involved people, they could vote by mail, and we have made that even easier. But they had actual paper ballots that they did, and then they were fed into this machine to count with auditing. But you are right. That is what people were talking about. Why can't you just do it from your home computer and have no back-up, right?

Mr. SCHOELLER. Right. That was one of the things I actually had to disagree when that viewpoint was put forth, particularly in one

city I remember. Even after I became elected, I went to a conference of other elected officials, and there was a group of speakers, and they all were talking about this. There was actually one speaker——

Senator KLOBUCHAR. Like voting from Facebook.

Mr. SCHOELLER. Correct.

Senator KLOBUCHAR. Just kidding. That was a little——

Mr. SCHOELLER. But they actually disagreed, and I went up and I think I was the only election official that day—this was prior to 2016—that didn't think that was a good idea. But I think we have evidence now from 2016 that clearly that is a convenience that we just can't afford.

Senator KLOBUCHAR. Very good. Mr. Schoeller, in your testimony, you supported the Secure Elections Act's increase of cybersecurity expertise, what is currently the Technical Guidelines Development Committee. Additionally, you support even more robust auditing provisions.

Mr. SCHOELLER. Yes.

Senator KLOBUCHAR. We talked about that, and so you think that that is very important to have this post-election audit. Correct?

Mr. SCHOELLER. I do. Certainly—and one of the things I wanted to recognize is when we do these audits, they are very transparent. They are very open to the public, and that is something that you could not put a value on.

Senator KLOBUCHAR. Mr. Praetz, thank you for supporting the Secure Elections Act in your testimony, and I think it must be hard to be always used as the example of Illinois, that they got that close. But it must make it more of a concern in your state when you know that happened.

Mr. PRAETZ. Yes. Certainly. It hits home.

Senator KLOBUCHAR. Very good. Are people aware of it, do you think?

Mr. PRAETZ. Oh, yes. I mean, you know, our voters come to us, and we are lucky in Illinois because we can tell a strong story. We start at the end. We have got a piece of paper that every voter looked at. Worst-case scenario, a Sony-type attack with full meltdown of all systems, we can re-create an election that is trusted and true.

Do you want to keep talking about election security? Most people walk away. Some will engage.

If we were able to talk that way nationally, this would be probably the last hearing of this sort we will have. I mean, it is a very effective narrative.

Senator KLOBUCHAR. Yes. Do voters get worried about having their private data taken?

Mr. PRAETZ. Sure. Certainly.

Senator KLOBUCHAR. Which is a different issue, of course, than trying to tamper.

Mr. PRAETZ. It is an entirely different issue.

Senator KLOBUCHAR. I mean, it could happen at the same time, but it is a different concern.

Mr. PRAETZ. Now, luckily, we have the datasets we keep on voters don't have a tremendous amount of PII, but it is certainly something that we protect.

Senator KLOBUCHAR. Of course, we have been talking about the fact that Homeland Security didn't come forward with the information to the state. When did you find out about the—

Mr. PRAETZ. Well, so, again, it happened at the state level, and I know as much as anybody else from the 60 Minutes story. They shut down the statewide voter registration system sometime in the summer, and then we started asking questions.

We are a bottom-up state. Each county in Illinois has their own voter registration system, and then we share data up to the State Board of Elections, which also is another sort of resilient policy choice because even if the state board system had been taken down, we would all have been to operate pretty seamlessly.

Senator KLOBUCHAR. I think there is just a secondary concern that people aren't always focused on is that the hacking could also result in stealing of private voter information.

Mr. PRAETZ. Of course.

Senator KLOBUCHAR. The people's addresses, stuff like that. We have been talking a lot about DHS, but you both mentioned EAC briefly in your testimony, and could you talk about the role that the Election Commission has played in improving communications around cybersecurity?

Mr. PRAETZ. Certainly. I sit on the Executive Committee of the Government Coordinating Council, and I sit alongside the chairman of the EAC and the president of NASS and NASED, and this sort of confederation is working really well to—for all of us to sort of figure out our lanes. What has become clear to everybody, including Homeland Security, is the vital role that EAC has played. For 15 years, they have been a significant partner. They are a trusted source. I think DHS has been able to rely on them significantly, and we have certainly at the local level.

Senator KLOBUCHAR. Mr. Praetz, you discussed cyber navigators extensively in your testimony, and Mr. Schoeller mentioned that not all election authorities have access to a team dedicated to protecting them, which you noted. Can you both discuss how cyber navigators can provide local election officials with a much-needed resource and expertise?

Mr. SCHOELLER. I think that is the issue. You mentioned the EAC. You know, they have a number of white papers. They have a number of information that is out there available. They are trying to do all they can.

I think the issue, and this is in my broader testimony that I have included for the record, is that oftentimes a local election official, they are so overtasked with all these various administrative duties, they don't have a budget to be able to handle the duties they have, they don't have access to that information just by the logistical way their job occurs every single day.

That is why I think if we can have programs that are there to help, like Noah mentioned this morning, I think that is going to be the type of help that our local election officials appreciate. Because they are concerned. They are worried. They realize they don't

have the technical background or capabilities or the local help to be able to get that protection they need.

One of the things that I want to mention, I think the other issue is that sometimes they will go out to somebody there locally to get help. But how do they know if the help they are being provided is what they need? I think that is another thing, and part of helping educate local election officials is, okay, this is a product or this is a company you can trust.

I mean, we get a lot of information from companies, you know, telling us they will help us in terms of cybersecurity, but what product is actually really needed versus what would we just be spending money on that would be frivolous and not really protect us at the end of the day?

Senator KLOBUCHAR. Very good. Thank you to both of you.

Chairman BLUNT. My last question for both of you, and there may be questions in writing, do you see any potential for unnecessary duplication with the EAC and the new involvement of Homeland Security? If you do, is there a way we can thoughtfully try to deal with that?

Mr. PRAETZ. I have no concerns there. I think Homeland Security has got quite a broad plate of responsibilities. Now I am glad that they are able to share some of their cyber-specific resources. I think it is critical to have an institution dedicated solely to election support that will not get pulled into other issues.

Chairman BLUNT. Mr. Schoeller?

Mr. SCHOELLER. I think the issue is broad enough that the coordination is good, and I think the EAC terms of the other areas they help out with in terms of the clearing house for best practices of the local election official, those types of things they provide that DHS is not going to provide. But I think when it comes to protecting ourselves in terms of the cyber world, I don't think you can be too broad at this point.

Chairman BLUNT. As an interface, you would be comfortable reporting things to EAC that then they would report on to Homeland Security if they decided necessary?

Mr. SCHOELLER. Yes.

Mr. PRAETZ. That is correct. We didn't sort of in the information-sharing protocols that the GCC has developed, that is not the exact design, but I have zero doubt that the officials at the EAC and the DHS that are working on this will share information appropriately with each other.

Chairman BLUNT. Well, thank all of you. We have started a couple of votes that we are going to need to go to, but we appreciate you and the other witnesses being with us today.

The record will be open for a week from today, and there may be some questions that come to you in writing. If they do, we would hope you would respond to those as quickly as possible.

[The information referred to was submitted for the record.]

Chairman BLUNT. The hearing is closed.

[Whereupon, at 12:38 p.m., the hearing was adjourned.]

APPENDIX MATERIAL SUBMITTED

Written Testimony of John R. Ashcroft

Missouri Secretary of State

United States Senate Committee on Rules and Administration

June 20, 2018

Thank you, Chairman Blunt and distinguished committee members, for the opportunity to join you here today for this important discussion regarding the security of our elections. My name is John Ashcroft, and it is my distinct privilege and honor to serve as the 40th Secretary of State for the great people of the state of Missouri. Notably, this is an office administered at one time by the chairman of this committee.

I decided to run for secretary of state because of my four children. My goal was to ensure their voices and those of future generations would continue to be heard at the ballot box. One of the priorities of my campaign was to enact legislation that both increased the security of our votes and made sure that every registered voter could vote. Simply put, in Missouri, "if you're registered, you can vote, and your vote will count."

Elections are the bedrock of our democratic republic, as they are how we the people consent to be governed. The integrity of these elections is of the utmost importance every day when I go to my office in Jefferson City, and I know my fellow election officials across the country share that same concern and dedication.

I welcome today's conversation to talk about election security preparations, but before we move forward, we should briefly look back to the impetus of why we are all here today: Allegations that outside actors threatened the integrity of our elections during the 2016 election cycle. While these are serious allegations, it is vitally important to understand that after two years of investigation, there is no credible evidence that these incidents caused a single vote or voter registration to be improperly altered during the 2016 election cycle. It was not our votes that were hacked, it was the perception that was hacked.

Secondly, every reported cyber incident in 2016 involving state election systems was first detected by state election authorities. In each case, election authorities brought the incident to the attention of federal authorities, not the other way around.

This is not to say that our elections are perfect, that there was no fraud, that there were no unlawful corruptions of votes or vote totals. The evidence indicates that voter fraud is an exponentially greater threat than hacking of election equipment. In 2010, well before elections being altered rose to the forefront of the public conversation, there was a race for a Missouri state house seat that was decided by one vote. Yes, just one vote. Election authorities conclusively determined in that election that there were two voters (who also happened to be family members of the victorious candidate) that voted illegally. Despite the fact that the candidate's relatives admitted to illegally voting and ultimately pled guilty to their election offenses, their nephew now serves in the Missouri Senate.

Consequently, moving forward, any meaningful enhancement to election security must take a comprehensive approach to ensure that every legally registered voter is allowed to vote and that their vote is not diluted by any sort of voter fraud, malfeasance, or ineptitude. Moreover, we must avoid knee jerk reactions that would give voters a false sense of security.

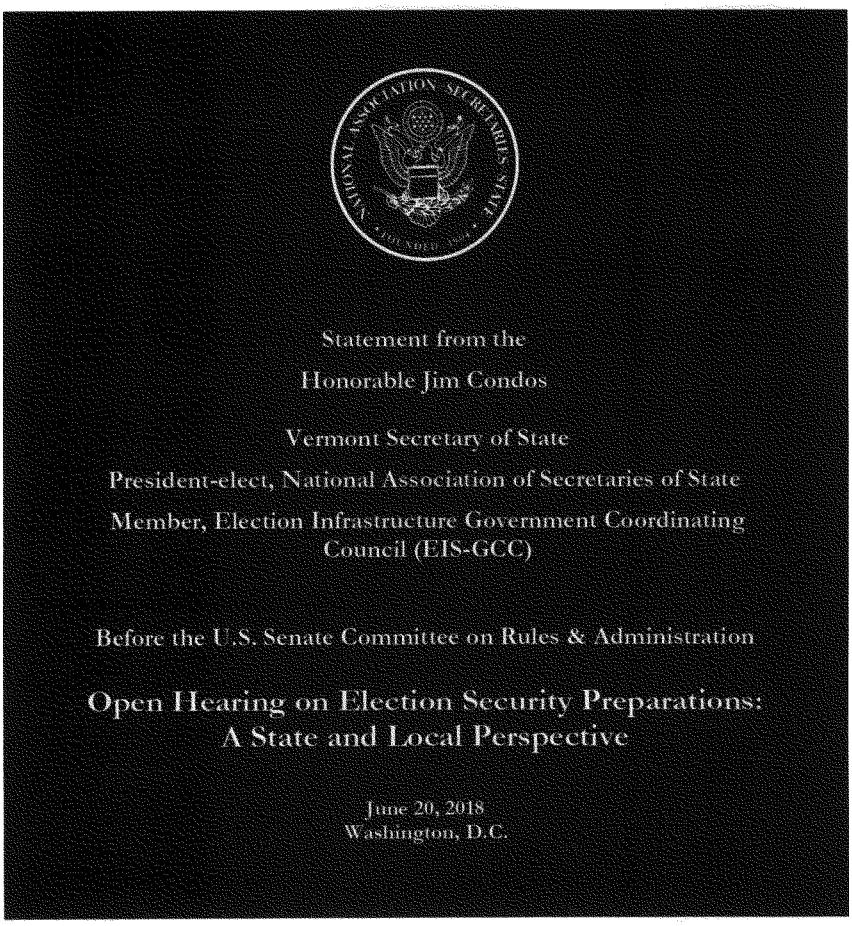
In its current format, the Secure Elections Act focuses on improving communication between federal agencies and states regarding cyber threats and election security. That is a good start. However any communication mandates must remedy the failure of federal agencies to communicate and work with local election authorities. States have and will continue to work with federal agencies regardless of any new legislation. However there is a longstanding problem of federal officials refusing to share valuable information with state election officials. The National Association of Secretaries of State has passed resolutions since 2012 calling on the federal government to meet its statutory obligations to share information with state election officials.

As important as this information sharing is, there are numerous other ways to protect our elections beyond information sharing.

Proposed changes should recognize the value of allowing state election officials to remain in control of elections. I have learned that winning an election does not make you an elections expert any more than watching a Fourth of July celebration makes you a rocket scientist. Time spent in the trenches on Election Day, as an official or as a poll worker, is what make one an expert, and legislation should respect that.

I'll close by noting to a certain extent the irony of the time in which we are are living. A little over a decade ago, in the wake of the last period of heightened national interest in the administration of this country's elections, at hearings just like this, the all-knowing federal government assured elections experts that all that we needed to do was switch to electronic voting equipment. It was the determination, in the wake of the 2000 presidential election, that the use of electronic voting equipment was the only way to guarantee every American vote was accurately reflected in the election results. Now, the same all-knowing federal government is telling election experts to stop using electronic equipment; that paper is the only way to truly verify election results.

Working together, it is my hope that we can forge a comprehensive framework of protections to enhance our sacred democracy. Thank you very much.



National Association of Secretaries of State
444 North Capitol Street, NW – Suite 401
Washington, D.C. 20001
202-624-3525 Phone/202-624-3527 Fax
www.nass.org

Hon. Jim Condos, Vermont Secretary of State
Statement Before the U.S. Senate
Committee on Rules & Administration
June 20, 2018 | Washington, D.C.

NASS
National Association of Secretaries of State

My name is Jim Condos, and I am Vermont's Secretary of State. I am also president-elect of the nonpartisan National Association of Secretaries of State (NASS), and a member of the Department of Homeland Security's Election Infrastructure Subsector Government Coordinating Council (EIS-GCC). I will become the new NASS president on July 16, 2018, and I have every intention of continuing the positive work of current president Secretary Connie Lawson of Indiana, and those that served before her. NASS is fortunate to have outstanding leaders and I am proud to be a part of the association.

Thank you for the chance to appear before you today to join my colleagues and address some of the things happening at the national level, some work specific to Vermont, and also my goals for NASS and the Election Infrastructure Government Coordinating Council as I become the President of NASS when Secretary Lawson's term ends in mid-July.

In March 2018, I had the privilege of testifying before the U.S. Senate Select Committee on Intelligence regarding election security.

Primary elections across the country are well underway, with states administering elections in a secure, accurate, and fair manner.

I. STATE AND FEDERAL PARTNERSHIP EFFORTS TO SECURE ELECTION INFRASTRUCTURE

State and local election officials and the federal government have worked very hard to create a productive relationship since former DHS Secretary Jeh Johnson announced the "critical infrastructure" designation for election systems in January 2017. As you may know, NASS and its members raised many questions and expressed serious concerns about the potential federal overreach into the administration of elections – a state and local government responsibility.

While we remain vigilant about possible federal overreach, we will work together to ensure that the "critical infrastructure" designation functions in a positive and effective way. Thus, we have chosen to actively focus on improving communication between the states and the federal government to achieve our shared goal of securing elections. In particular, we have utilized the Election Infrastructure Subsector Government Coordinating Council (EIS-GCC), which Secretary Lawson mentioned in her testimony, to open communications channels and guide future collaborative election security endeavors.

For instance, within the EIS-GCC's Subsector Specific Plan, there are many short and long-term goals and projects to support election officials, federal partners and stakeholders. These include deploying an online training environment for election officials, identifying resource gaps at the state level, and establishing a digital portal to increase communication between all levels. Many of these will be discussed at the July EIS-GCC meeting in Philadelphia. At that meeting, we will also begin important discussions with the Elections Infrastructure Sector Coordinating Council. This is the council that represents the private sector and non-profit sector stakeholders that support election officials.

As I transition to NASS president in less than a month, I will also take Secretary Lawson's place on the

EIS-GCC Executive Committee. It is my objective to continue Secretary Lawson's vital work with this group on behalf of NASS.

However, I would be remiss if I didn't point out many of the organizations that have eagerly stepped up to help state and local governments with their election security efforts. NASS focuses a great deal on election security; and our meetings are replete with shared practices from our colleagues around the country including presentations by security and audit experts. We also hold forums twice a year for our office CIO/CISOs to come together to discuss challenges and solutions. The Belfer Center has developed a Tabletop Exercise that we can implement in our states to train both state and local election officials on addressing challenges leading up to and on Election Day. The Center for Internet Security has developed a handbook of election cybersecurity best practices and a checklist for states to monitor their progress. The Democracy Fund is supporting the convening of state and local officials to improve communication and governance between state agencies, and between state and local governments. And private sector companies like Google and Cloudflare have stepped up to provide free resources to state and local governments to assist with preventing distributed denial-of-service (DDos) attacks and protecting our data and websites. The list truly goes on, but my time is limited.

II. STATE SPECIFIC EFFORTS TO SECURE 2018 AND 2020 ELECTIONS

In regards to specific state preparations for 2018 and beyond, I would like to thank you and your colleagues for appropriating the remaining Help America Vote Act (HAVA) funds to states in the recent omnibus bill. We truly appreciate this money and it will go a long way in helping states strengthen and improve their elections systems. While our upgrades to equipment and cybersecurity improvements will be an ongoing challenge, and for many states the federal funding received will regrettably be insufficient to do all that they want and need, we are grateful for the boost that these federal funds provide.

In Vermont, we have already requested and received our $3 million grant of HAVA dollars from the U.S. Election Assistance Commission (EAC), which as the Vermont Secretary of State I believe the EAC has done a great job of dispersing these funds. And because of this and their positive work as a whole, I believe they should receive any resources needed moving forward.

In regards to specific plans in using these new HAVA funds, in Vermont we plan to:

- Implement, prior to Vermont's 2018 Primary, two factor authentication for our local clerks and SOS staff to access our Election Management System
- Implement, prior to Vermont's 2018 primary election, a new user-friendly ADA compliant Accessible Voting System that will allow voters with disabilities to vote privately and independently at the polling place and from home during the early voting period
- Conduct an additional round of penetration testing on our election management system by an independent vendor this spring and will do so at regular intervals going forward
- We have offered an online cyber-security training webinar to our local clerks and will continue to offer additional rounds of these at regular intervals going forward
- Following the 2018 General election and every General election going forward we will perform

a robust audit of our election results using state-of-the-art auditing technology
- Prior to 2020 Election, new Vote Tabulators with Paper Ballot and Audit Capabilities

This plan is in addition to what we are already currently doing, including:
- Continued improvements to our cyber defense
- Mandatory election trainings to Vermont's municipal clerks
- Cyber summit convening state and local partners to inform Vermonters of our efforts and build confidence in the integrity of our process

BACKGROUND ON VERMONT'S ACTIONS SECURING OUR ELECTION INTEGRITY

My agency began a thorough review of its cyber posture in 2013, when we issued an RFP for both physical and cybersecurity risk assessments which was completed in 2014. In the fall of 2015, we completed implementation of a new election management platform which included a vulnerability assessment and penetration testing prior to deployment. This new system provides:
- A statewide voter registration database
- Statewide absentee ballot request and tracking system
- Election night reporting
- Canvassing and official results reporting
- Online voter registration and My Voter Page
- Ballot production

Over the past four years, my office has overseen reforms of Vermont's voting laws and process which simultaneously improve the integrity of our elections and encourage voter participation and access to elections. These include:
- Expansion of No Excuse Early/Absentee Voting for 45 days before the election
- Online Voter Registration and the My Voter Page
- Election Day registration and elimination of a pre-election registration deadline
- Automatic Voter registration at the DMV

Some of the acknowledged "best practices" that Vermont already uses include:
- Paper ballots
- Post-election audits
- No internet (Wi-Fi or hard-wire) connection of our vote tabulators
- Daily backup of our voter registration database
- Daily monitoring of traffic to our site
- Blacklisting of known problem or suspected IP addresses
- Periodic Penetration Testing
- "Secure the Human" training for Vermont's municipal clerks

We have no less than three firewalls between the outside internet and our cyber systems as well as:

- Joining the Election Infrastructure – Information Sharing Analysis Center (EI-ISAC)
- Installation of a real-time Albert monitor (MS-ISAC)
- Receiving weekly DHS cyber-hygiene scans
- Contacts with both DHS and FBI personnel

I can elaborate further during the question and answer portion of this hearing or anytime in the future.

III. THE FUTURE OF ELECTIONS AND VOTER CONFIDENCE

Much of the national attention over the past 18-24 months has focused on election security issues – especially cybersecurity – which are of course, extremely important. If people are confident that the voting process is secure, they will be much more likely to participate. This is why we need members of this committee, DHS and our other federal partners to share with Americans that our elections are indeed secure, accurate and fair.

The risks to our election system are real and we have and will continue to address them appropriately. However, it is important to understand that those systems with the highest risk – online voter registration systems and election night reporting are removed from the process of casting a ballot. It is also important to recognize that requiring a paper ballot with a robust post-election audit should be considered critical.

If our protections to our voter registration system are breached, we can address that and the vote count is not impacted. If our protections to our website posting election night reporting are breached, we can address that and the vote count is not impacted.

Voter confidence may be impacted, and that is not insignificant, but they need to understand that the casting of a vote is separate from all these other parts of the system. While we all need to work together to combat misinformation – intentional and accidental - to maintain voter confidence, I also encourage those citizens watching today to get involved in the process by becoming a poll worker, reaching out to their state and local election officials with questions, and ultimately casting a vote in November.

In the meantime, please know that state election officials will continue their work to increase cybersecurity and run elections with the utmost integrity. The 2018 election will be a test of what we learned from 2016. I feel that we are ready for 2018 and as the next president of NASS and as Vermont's Secretary of State I will continue to focus on improvement as time marches forward.

Your vote is your voice!

Thank you again, Members of this Committee for inviting me and my peers to testify before this hearing and for giving me the opportunity to speak about this important matter on behalf of NASS and Vermont.

I look forward to answering any questions you may have for me.

Testimony of Minnesota Secretary of State Steve Simon

U.S. Senate Committee on Rules & Administration
"Election Security Preparations: A State and Local Perspective," June 20, 2018

Mr. Chairman, Ranking Member Klobuchar and members of the committee:

Thank you for the opportunity to be with you today. I'm grateful for your willingness to engage on this vital topic, and I'm honored to be part of this bipartisan group of testifiers today.

Election security in general, and cyber security in particular is the most significant threat to the integrity of our election system. I've been in this job since January of 2015, and I'm sometimes asked by friends and family what my biggest surprise is about being Secretary of State. My answer is always the same: My biggest surprise is how much of my time and energy (and the time of senior staff) is spent on cyber security.

We are today faced with, not only the possibility, but the very real likelihood that some outside force will again target the instruments of our democracy for espionage or attack. This threat has become part of the American public's consciousness only in the last few years, most pointedly as a result of the activity surrounding the 2016 election. By now it's clear that this cyber security challenge is a race without a finish line. We have to stay at least one step ahead of the bad guys all the time – and without end. There is no tape to cross, and no end zone where we can spike the football.

The good news is that Minnesota and other states are more prepared than ever before to confront the threat.

My office began to accelerate our election security work in early 2015. We formed an IT Security Team. We dedicated staff specifically to the modernization and re-coding of existing systems, including our Statewide Voter Registration System, we wrote an emergency response plan, we worked closely with our partners at the county and city levels, and we contracted with a security outside consultant to provide us with an extra set of eyes and ears to explore our possible vulnerabilities. We believe that these efforts paid off in August 2016 when foreign actors tested our defenses, and we expect that our ongoing efforts will be tested again this election year.

According to US Intelligence officials, Minnesota was one of the 21 states in 2016 targeted by hackers acting at the behest of the Russian government. We didn't learn the specific nature of the attempted intrusion until ten months after the fact, which is when the Department of Homeland Security briefed me, but we know when and how we turned back all attempts to infiltrate our system. Two of the 21 targeted states found themselves in a different position; victims of an actual breach.

With the 2018 election rapidly approaching - Minnesota's primary is in 55 days and our early voting period opens in just 9 days - I am feeling cautiously optimistic. We believe that we are even better prepared than in 2016 - for several reasons:

- First, the design of our system is sound. We are a paper ballot state. We are proudly "old school." After a voter fills out a paper ballot, an election judge places the ballot in an optical scan machine. Results from the county and municipal levels are reported to my office via telephone before being uploaded by way of an encrypted system. We then have post-election audits by counties and post-election reviews by our office. The risk to an attack on our vote tally or outcome of our elections is very low and I am confident that votes of Minnesotans will be counted accurately.

- Second, we have benefited from the DHS "critical infrastructure" designation. After a rocky roll-out, that designation has been a success from our standpoint. It has not been an encroachment on state authority over elections, as some feared. It has not resulted in regulation, as some feared. On the contrary, it has provided us with expertise and resources. DHS has helped us, both in person and remotely, to identify potential vulnerabilities and best practices. We have either already implemented DHS suggestions - or we are in the process of implementing them.

- Third, DHS has put together a Government Coordinating Council (on which I sit) to harmonize efforts among various levels of government. For example, the GCC is set to finalize communications protocols so that various units of government encountering possible threats or cyber-incidents can communicate with other units of government.

- Fourth, we now have the attention of you in the Congress, of our state legislature, of the news media, and most importantly, of the American public. Everyone now seems to understand the high stakes.

In Minnesota, the stakes are particularly high because we are the #1 state in voter turnout - with a total turnout of 74.7% of eligible voters casting ballots in 2016. Our people are doers, joiners, and voters. Sometimes I get asked why Minnesota's voter turnout is so high. I think a few factors contribute, but among them is the high level of confidence that people in Minnesota have in the integrity of our system. Failure to confront election security in general (and cybersecurity in particular) would put that high level of confidence at risk.

These are tough challenges. No election administrator can responsibly say that there is no risk of a breach. I can't do that, and I won't do that. There is always the possibility of a breach. But in Minnesota we are optimistic about the active measures we have taken to meaningfully reduce the risk.

I would like to say a word about the funds that you appropriated in late March for state election security measures, as part of the omnibus budget bill. The amount was over $380 million, of which our share in Minnesota is $6.6 million. That money will enable us to continue to implement DHS recommendations, to buy software and hardware, and to hire people to secure and modernize our system. At a time when many spending decisions fall victim to partisanship and politicking, it is a strong statement that this funding had broad bipartisan support. I want to specifically thank my senator, Senator Amy Klobuchar, for her efforts and that of her colleagues. Your attention to this issue – truly to defending democracy –will make a lasting and positive difference.

In Minnesota, unfortunately, we'll have to wait a bit. Our state law requires that even when federal money is made available to us, we need to obtain legislative approval to access the funds. We sought two sentences of authorization language from the legislature this year, but some legislative leaders chose to take a risky path – with the predictable and utterly avoidable result that the authorization language did not survive the legislative process. So, we will have to wait to use that money until after the 2018 election – presumably when the legislature convenes next January.

Going forward, we will continue to need your partnership.

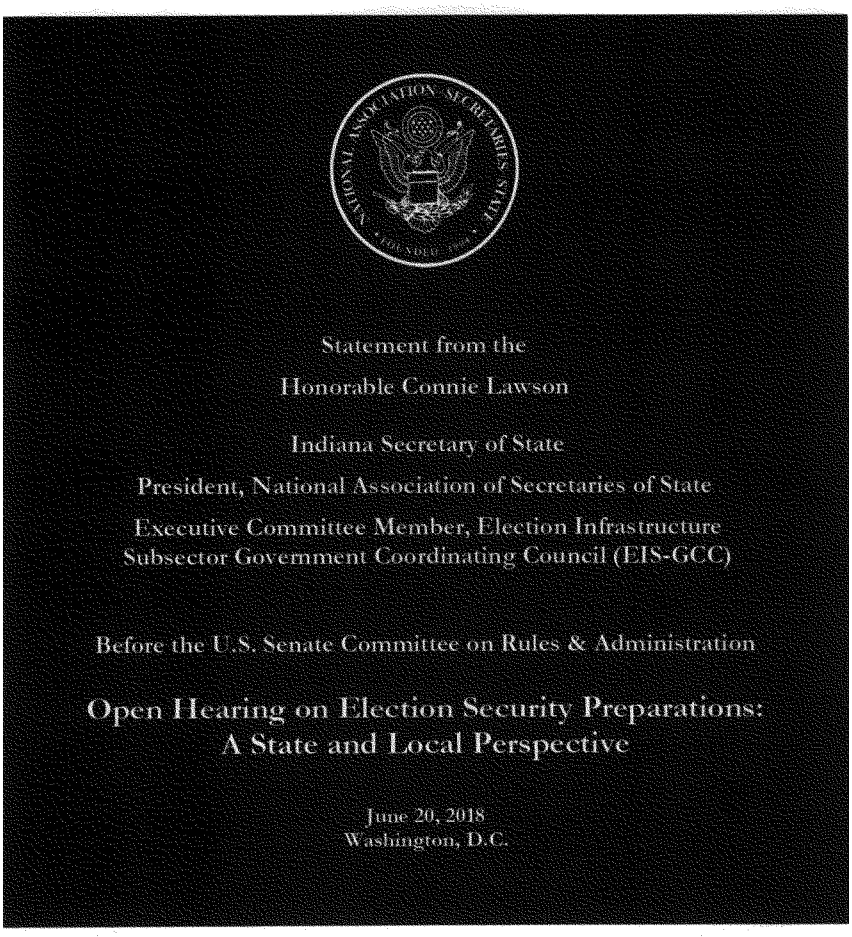
We will need resources to strengthen and extend the protections to our election security. More software, hardware, and human expertise will be essential. And expensive. Any ongoing federal resources would be appreciated – and would be put immediately to work.

We would also benefit from expertise. To that end, I urge support for the Secure Elections Act. I had the privilege of joining my Senator (Senator Klobuchar) along with Senator Lankford (and a few other Secretaries of State) recently in the Capitol Building to provide feedback on the legislation. I do support the bill. It recognizes the very real threat that we face; the threat that you and your colleagues have already acknowledged. It would provide floors (not ceilings) for state action to secure elections. It would provide guidelines and best practices that reflect the very real federal interest in ensuring that all elections in all of the states are administered with care and skill. I think the latest version of the bill strikes the right balance – by ensuring state control of elections, but with reasonable and measured help from the federal government.

I like to say that I am in the democracy business. As United States Senators, there are few who truly understand and live this concept as completely as you. This is where serious business is done for the American people -- and there is nothing more serious in the 21st Century than defending democracy; defending the American way of life. Strong forces around the world seek to undermine us at every turn. I will continue to urge this body to put country over party, as you did when you made available these election

security funds. I am depending on your continued investment, as are my fellow Minnesotans and our fellow Americans.

Again, thank you for inviting me to testify today. I look forward to our continued partnership.



Statement from the

Honorable Connie Lawson

Indiana Secretary of State

President, National Association of Secretaries of State

Executive Committee Member, Election Infrastructure Subsector Government Coordinating Council (EIS-GCC)

Before the U.S. Senate Committee on Rules & Administration

Open Hearing on Election Security Preparations: A State and Local Perspective

June 20, 2018
Washington, D.C.

National Association of Secretaries of State
444 North Capitol Street, NW – Suite 401
Washington, D.C. 20001
202-624-3525 Phone/202-624-3527 Fax
www.nass.org

Good morning, Chairman Blunt, Ranking Member Klobuchar and distinguished Members of the Committee. Thank you for the chance to appear before you today my name is Connie Lawson, and I am the Indiana Secretary of State. I am also president of the bipartisan National Association of Secretaries of State (NASS). In addition, I am a member of the Executive Committee of the Election Infrastructure Subsector Government Coordinating Council (EIS-GCC).

I was invited here today to testify as NASS President. I am honored to represent our nation's Secretaries of State, forty of whom are their state's chief election official. NASS is an organization made up of bipartisan officials, but when we speak as an organization, we speak with one voice.

I am delighted to join my colleagues to showcase what we are doing to prepare for the 2018 election cycle and beyond. As you know, we are in the midst of primary season, with state and local election officials administering successful and secure elections. I would like to take this opportunity to reassure this committee and voters alike that we have worked tirelessly to further safeguard the elections process by working with our local election officials, our IT teams, private sector security companies, the federal government and various stakeholders.

I. ELECTION INFRASTRUCTURE SUBSCECTOR GOVERNMENT COORDINATING COUNCIL (EIS-GCC) EFFORTS

The 2016 election cycle highlighted challenges in communication and the sharing of information between the Department of Homeland Security (DHS) and the states. We learned in 2017 that a number of state systems were scanned and probed leading up to November 2016 by bad actors trying to access our voter registration systems and websites. However, it is important to note that **no votes were changed** in 2016 and federal, state and local officials have tackled the communications challenges head on. We are taking the lessons learned from 2016 and Secretaries of State are focused on moving forward. We have done so by working together and with our federal partners like DHS, the U.S. Election Assistance Commission (EAC) and through the Election Infrastructure Subsector Government Coordinating Council (EIS-GCC). The EIS-GCC was established in October 2017 to enable improved communications between state and local officials and the federal government and to share resources. The EIS-GCC is comprised 29 members, of which 24 are state and local election officials. This is the first group of its kind and helps us stay on the same page and share vital information.

Since the EIS-GCC was established there have been two in-person meetings, October 2017 and February 2018, with another in-person meeting happening July 13, immediately before our NASS Summer Conference in Philadelphia, Pennsylvania. The EIS-GCC currently has nine working groups that address the goals and the mission of the GCC and an Executive Committee made up of 5 members (President of NASS, President of NASED, DHS rep, EAC rep and local official rep.) The Executive Committee meets every two weeks via conference to review working group progress and materials, discuss communications strategy, track sector progress and plan for future work products. For example, we are in the final stages of approving the Communications Protocol Framework, which outlines how state and local election officials share information with DHS, FBI and ODNI, and vice-versa.

The EIS-GCC has also been developing our Sector Specific Plan. This document will undergo a final review at our July 2018 meeting and if approved, it will be included in the National Infrastructure Protection Plan (NIPP).

Additionally, through the work of the EIS-GCC a number of states participated in a pilot program to share election-specific threat indicators. From that pilot, a full Election Infrastructure Information Sharing and Analysis Center (EI-ISAC) has become operational. States will have the option to put monitors on their election-networks to track traffic, detect anomalies and share with other states.

This work has created a solid foundation for the EIS-GCC to have frank and productive conversations as we all work to ensure the security of the nation's elections.

II. FEDERAL FUNDS FOR ELECTION SECURITY

The members of NASS are extremely pleased that the Consolidated Appropriations Act of 2018 included $380 million of Help America Vote Act (HAVA) funds. This funding will help states further prepare for elections by increasing cybersecurity, replacing aging voting equipment, educating voters and much more.

When it passed in 2002 HAVA was the first piece of federal legislation to provide funding for election administration improvements, and states used the opportunity to enhance the security, accessibility, accuracy and reliability of election systems. Implementation of HAVA was a success, and it helped improve the voting experience for all Americans over the last 15 years.

While it may seem like this funding was delivered in time to see physical changes for November 2018, that will often not be the case. Most states will have implemented security and data protection improvements and policy behind the scenes including vulnerability testing, IT staff recruitment, risk mitigation solutions and training. However, states that are utilizing these federal funds to purchase new voting systems and equipment upgrades will likely not have much in place for this election. The HAVA funding appropriated will make a difference in the upcoming 2018 elections but will be much more visible by 2020.

There are several things that states want or need to do before spending this money. Many need sign-off from their legislatures that already have or soon will be adjourning. Others are convening stakeholders to get input on priorities, and more are meeting with local officials to understand their most pressing needs. Federal funds are rare and it is imperative that these new funds are used judiciously.

It is important to remember that certain enhancements can be done quickly, but others require careful planning, requiring gathering of information and slow implementation. According to the EAC, as of June 8, 2018 59% of HAVA funds have been requested by 29 States. States will submit plans and budgets to the EAC outlining the intended use of their new federal funds. Each state's plan will look different. My colleagues testifying before you today can speak about their priorities for their HAVA dollars.

In Indiana, we are meeting with local election officials and stakeholders to determine the best use of the funds. We understand this is a one-time limited infusion so we are doing our due diligence to ensure the funds are utilized in the most effective manner. Indiana appreciates the need for network security around all election equipment. In doing so we are considering virtual private networks for our ePollBook connections and county based Albert sensors. As emphasized by the FBI in 2016, multi-factor authentication is one of the most critical tools of cyber defense. As a result, this spring, we conducted a two-factor authentication pilot with 10 of Indiana's 92 counties. The pilot introduced a physical USB tokens and a unique identifier to access the Statewide Voter Registration System. Additionally the pilot restricted access to working hours for each employee, which could be adjusted by county administrators. We learned a lot from this program and hope to expand it statewide.

Even though this journey will take time, please understand that election officials work to ensure that elections are administered in a secure manner, whether it's protecting voter registration data from cybersecurity threats or ensuring that the votes cast are protected from tampering or manipulation. As election officials work to fulfill this commitment to improve voter confidence, we are glad that Congress fulfilled its commitment to states and fully funded HAVA. Please know that states look forward to using this money judiciously in the coming months and years to help protect the nation's election infrastructure.

III. THE 2018 ELECTION CYCLE AND BEYOND—SECURING ELECTIONS AND RESTORING VOTER CONFIDENCE

Secretaries of State and their staffs are also working with their state legislatures to secure additional funding for improved cybersecurity, new voting machines, additional IT staff and to strengthen existing election systems.

In Indiana, we have migrated data, which has created more tailored services as a result of our unique election needs. Our outward facing websites and electronic poll books work on a mirror of the actual database, thereby mitigating and limiting potential for damage as a result of unauthorized access. We have also taken advantage of free services offered by DHS including cyber hygiene, risk and vulnerability testing and penetration testing. We have also done internal phishing campaigns to educate staff and counties. Earlier this month, we did our first risk-limiting audit in Marion County, which includes Indianapolis. The pilot went well and we are working to develop audits in each county. On Primary Election Day, we had cyber teams in place monitoring activity. I am pleased to report we did not see anything suspicious.

This will be an ongoing commitment by state and local election officials and our federal partners. It is my hope my testimony has provided you with many concrete examples of how we have taken positive steps to move forward from 2016. I look forward to continuing this journey with my colleagues and having a successful mid-term election.

In conclusion, NASS and its Members ask that Congress, DHS and others such as the EAC, help us in

this process and work with us to further restore the nation's confidence in our elections.

I want to again thank the Members of this Committee for holding this hearing and giving me the opportunity to speak about this important matter on behalf of NASS.

I look forward to answering any questions you may have for me.

Statement for the Record

Matthew Masterson
National Protection and Programs Directorate
U.S. Department of Homeland Security

FOR A HEARING ON

"Election Security"

BEFORE THE
UNITED STATES SENATE
COMMITTEE ON RULES AND ADMINISTRATION

Wednesday, June 20, 2018

Washington, DC

Chairman Blunt, Ranking Member Klobuchar, and members of the Committee, thank you for today's opportunity to testify regarding the U.S. Department of Homeland Security's (DHS) ongoing efforts to assist with reducing and mitigating risks to our election infrastructure. DHS is eager to share with you the progress we have made to establish trust-based partnerships with our Nation's election officials who administer our democratic election processes.

Recognizing that the 2018 U.S. mid-term elections are a potential target for malicious cyber activity, DHS is committed to robust engagement with state and local election officials, as well as private sector entities, to assist them with defining their risk, and providing them with information and capabilities that enable them to better defend their infrastructure. Safeguarding and securing cyberspace is a core homeland security mission.

Given the foundational role that elections play in a free and democratic society, in January 2017 the Secretary of Homeland Security designated election infrastructure as a critical infrastructure subsector. Under our system of laws, federal elections are administered by state and local election officials in thousands of jurisdictions across the country. These officials manage election infrastructure and ensure its security and resilience on a day-to-day basis.

As such, DHS and our federal partners have formalized the prioritization of ***voluntary*** cybersecurity assistance for election infrastructure similar to that which is provided to a range of other critical infrastructure entities, such as financial institutions and electric utilities.

Since 2016, DHS's National Protection and Programs Directorate (NPPD) has convened federal government and election officials regularly to share cybersecurity risk information and to determine an effective means of assistance. The Election Infrastructure Subsector (EIS) Government Coordinating Council (GCC) has worked to establish goals and objectives, to develop plans for the EIS partnership, and to lay the groundwork for developing an EIS Sector-Specific Plan (SSP). GCC representatives include DHS, the Election Assistance Commission (EAC), and 24 state and local election officials. Participation in the council is entirely voluntary and does not change the fundamental role of state and local jurisdictions in overseeing elections.

The Department and the Commission have worked with election industry representatives to launch an industry-led Sector Coordinating Council (SCC), a self-organized, self-run, and self-governed council with leadership designated by the sector membership. The SCC serves as industry's principal entity for coordinating with the government on critical infrastructure security activities and issues related to sector-specific strategies, and policies. This collaboration is conducted under DHS's authority to provide a forum in which government and private sector entities can jointly engage in a broad spectrum of activities to coordinate critical infrastructure security and resilience efforts which is used in each of the critical infrastructure sectors established under Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience*. The process is a well-tested mechanism across critical infrastructure sectors for sharing threat information among the federal government and critical infrastructure partners, advancing risk management efforts, and prioritizing services available to sector partners in a trusted environment.

NPPD also engages directly with election officials—coordinating requests for assistance, risk mitigation, information sharing, and incident coordination, resources, and services. In order to ensure a coordinated approach from the federal government, NPPD has convened stakeholders from across the federal government through an Election Task Force (ETF). The ETF serves to provide actionable information and offer assistance to assist election officials with strengthening their election infrastructure by reducing and mitigating cyber risk, and increasing resilience of their processes.

Within the context of today's hearing, I will address the unclassified assessment of malicious cyber operations directed against U.S. election infrastructure and our efforts to help enhance the security of elections that are administered by jurisdictions around the country.

Assessing the Threat

DHS regularly coordinates with the intelligence community and law enforcement partners on potential threats to the Homeland. Among non-federal partners, DHS has been engaging state and local officials, as well as relevant private sector entities, to assess the scale and scope of malicious cyber activity potentially targeting the U.S. election infrastructure. Election infrastructure includes the information and communications technology, capabilities, physical assets, and technologies that enable the registration and validation of voters; the casting, transmission, tabulation, and reporting of votes; and the certification, auditing, and verification of elections.

In addition to working directly with state and local officials, we have partnered with trusted third parties to analyze relevant cyber data, including the Multi-State Information Sharing and Analysis Center (MS-ISAC), the National Association of Secretaries of State and the National Association of State Election Directors. We also used our field personnel deployed around the country to help further facilitate information sharing and enhance outreach, which has resulted in the identification of suspicious and malicious cyber activity targeting election infrastructure. On October 7, 2016, DHS and the Office of the Director of National Intelligence (ODNI) released a joint statement on election security and urged state and local governments to be vigilant and seek cybersecurity assistance. Our message today remains the same.

Enhancing Security for Future Elections

NPPD is committed to ensuring a coordinated response from DHS and its federal partners to plan for, prepare for, and mitigate risk to election infrastructure. We understand that working with election infrastructure stakeholders is essential to ensuring a more secure election. NPPD and our stakeholders are increasing awareness of potential vulnerabilities and providing capabilities to enhance the security of U.S. election infrastructure as well as that of our democratic allies.

Election officials across the country have a long-standing history of working both individually and collectively to reduce risks and ensure the integrity of their elections. In partnering with these officials through both new and ongoing engagements, NPPD is working to provide value-added—yet voluntary—services to support their efforts to secure elections.

Improving Coordination with State, local Tribal, Territorial (SLTT) and Private Sector partners. Increasingly, the nation's election infrastructure leverages information technology (IT) for efficiency and convenience, but also exposes systems to cybersecurity risks, just like in any other enterprise environment. Just like with other sectors, NPPD helps stakeholders in federal departments and agencies, SLTT governments, and the private sector to manage these cybersecurity risks. Consistent with our long-standing partnerships with state and local governments, we have been working with election officials to share information about cybersecurity risks, and to provide voluntary resources and technical assistance.

The National Cybersecurity and Communications Integration Center (NCCIC) works with the MS-ISAC to provide threat and vulnerability information to state and local officials. Created by DHS over a decade ago, the MS-ISAC is partially funded by NPPD. The MS-ISAC's membership is limited to SLTT government entities, and all fifty states and U.S. territories are members. It has representatives co-located with the NCCIC to enable regular collaboration and access to information and services for state chief information officers.

Providing Technical Assistance and Sharing Information. NPPD actively promotes a range of services including:

Cyber hygiene service for Internet-facing systems: Through this automated, remote scan, NPPD may provide a report identifying vulnerabilities and mitigation recommendations to improve the cybersecurity of systems connected to the Internet, such as online voter registration systems, election night reporting systems, and other Internet-connected election management systems.

Risk and vulnerability assessments: We have prioritized State and local election systems upon request, and increased the availability of risk and vulnerability assessments (RVAs). These in-depth, on-site evaluations include a system-wide understanding of vulnerabilities, focused on both internal and external systems. We provide a full report of vulnerabilities and recommended mitigations following the testing.

Incident response assistance: We encourage election officials to report suspected malicious cyber activity to the NCCIC. Upon request, the NCCIC can provide assistance in identifying and remediating a cyber incident. Information reported to the NCCIC is also critical to the federal government's ability to broadly assess malicious attempts to infiltrate election systems. This technical information will also be shared with other state officials so they have the ability to defend their own systems from similar malicious activity.

Knowing what to do when a security incident happens—whether physical or cyber—before it happens, is critical. NPPD supports election officials with incident response planning including participating in exercises and reviewing incident response playbooks. Crisis communications is core component of these efforts, ensuring officials are able to communicate transparently and authoritatively to their constituents when an incident unfolds. In some cases, we do this directly with state and local jurisdictions. In others, we partner with outside

organizations. We recognize that securing our nation's systems is a shared responsibility, and we are leveraging partnerships to advance that mission.

Information sharing: NPPD maintains numerous platforms and services to share relevant information on cyber incidents. State election officials may also receive information directly from the NCCIC. The NCCIC also works with the MS-ISAC, allowing election officials to connect with the MS-ISAC or their State Chief Information Officer to rapidly receive information they can use to protect their systems. Best practices, cyber threat information, and technical indicators, some of which had been previously classified, have been shared with election officials in thousands of state and local jurisdictions. In all cases, the information sharing and/or use of such cybersecurity risk indicators, or information related to cybersecurity risks and incidents complies with applicable lawful restrictions on its collection and use and with DHS policies protective of privacy and civil liberties.

Classified information sharing: To most effectively share information with all of our partners—not just those with security clearances—DHS works with the intelligence community to rapidly declassify relevant intelligence or provide tearlines. While DHS prioritizes declassifying information to the extent possible, DHS also provides classified information to cleared stakeholders, as appropriate. DHS has been working with state chief election officials and additional election staff in each state to provide them with security clearances. By working with the Office of the Director of National Intelligence and the Federal Bureau of Investigation, in February 2018 election officials from each state received one-day read-ins for a classified threat briefing while they were in Washington, DC. This briefing demonstrated our commitment to ensuring election officials have the information they need to understand the threats they face.

Field-based cybersecurity advisors and protective security advisors: NPPD has more than 130 cybersecurity and protective security personnel available to provide actionable information and connect election officials to a range of tools and resources to improve the cybersecurity preparedness of election systems; and to secure the physical site security of voting machine storage and polling places. These advisors are also available to assist with planning and incident management for both cyber and physical incidents.

Physical and protective security tools, training, and resources: NPPD provides guidance and tools to improve the security of polling sites and other physical election infrastructure. This guidance can be found at www.dhs.gov/hometown-security. This guidance helps to train administrative and volunteer staff on identifying and reporting suspicious activities, active shooter scenarios, and what to do if they suspect an improvised explosive device.

Election Security Efforts Moving Forward

DHS has made tremendous strides and has been committed to working collaboratively with those on the front lines of administering our elections to secure election infrastructure from risks. The establishment of government and sector coordinating councils will build the foundations for this enduring partnership not only in 2018, but for future elections as well. We will remain transparent as well as agile in combating and securing our physical and cyber infrastructure. However, we recognize that there is a significant technology deficit across SLTT

governments, and State and local election systems, in particular. It will take significant and continual investment to ensure that election systems across the nation are upgraded and secure, with vulnerable systems retired. These efforts require a whole of government approach. The President and this Administration are committed to addressing these risks.

In closing, there is a fundamental link between public trust in our election infrastructure and the confidence the American public places in basic democratic functions. Ensuring the security of our electoral process is a vital national interest and one of our highest priorities at DHS. Our voting infrastructure is diverse, subject to local control, and has many checks and balances. As the threat environment evolves, DHS will continue to work with federal agencies, state and local partners, and private sector entities to enhance our understanding of the threat; and to make essential physical and cybersecurity tools and resources available to the public and private sectors to increase security and resiliency.

Thank you for the opportunity to appear before the Committee today, and I look forward to your questions.

Written Testimony

of

Noah Praetz
Director of Elections
Office of Cook County Clerk David Orr

before the

United States Senate
Rules and Administration Committee

Regarding

Election Security Preparations: A State and Local Perspective

June 20, 2018

Washington DC

Noah Praetz

Biography

Noah Praetz is the Director of Elections working under Cook County Clerk David Orr. He is responsible for the overall management of elections in Cook County, Illinois, one of the largest jurisdictions in the country. He believes that free and fair elections remain our core American value and organizing principle. Each year his team serves 1.5 million voters, facilitates democracy for thousands of candidates, and train and support thousands more volunteers to administer democracy.

He started as temporary worker hired to do data entry prior to the 2000 presidential election. In 2007 he became Deputy Director and in 2013 he was appointed Director.

Mr. Praetz is on the executive committee of the Government Coordinating Council representing the local election officials. He is the Treasurer of the International Association of Government Officials. He is also co-chair of the Election Center Cyber Security Committee. He is active in the Illinois Association of County Clerks and Recorders. He has presented on Election Security, Sustainability, Election Day Management, Online Registration, Voter Registration Modernization and other Election Related items.

Executive Summary

Election Officials have been securing our nation's votes and voter records for a very long time. We have been securing digital infrastructure for a more than a decade. But the changed environment and the expectation of continued sophisticated attacks forces us to up our game.

Spurred by the need to defend against foreign enemies, Federal and State officials have been working successfully to find a good balance of federal involvement in elections, without trampling on authority that the states zealously guard. Good progress is being made.

However, by and large, local election officials are the ones who control, secure, and run elections. We locals - 108 of us in Illinois and over 8,000 nationwide - are on the front lines of this new battlefield. We control almost the entire election infrastructure. We are the entities most in need of support and attention. We need help to fortify ourselves against the high probability threat actors we've been warned of.

In Cook County we have studied and undertaken significant efforts at securing our infrastructure and helping raise awareness within the ecosystem. We conclude that to decrease the likelihood of successful attack on digital services, each election official must have access to an election infrastructure security officer. Most locals don't have that capacity today.

Local election officials cannot master this problem without direct support of skilled experts. We suggest this be handled by a brigade of digital defenders, or what the government coordinating council calls "cyber navigators," supporting local election officials now and into the future.

These "navigators" should adopt the mantra of Defend, Detect, Recover. They need to accomplish these three vital goals. They can help improve defenses within election offices, following the specific recommendations of Center for Internet Security or Defending Digital Democracy -- we believe they'll quickly bring up the floor of the elections security ecosystem. They'll also establish detection techniques. And they'll develop recovery plans for when attackers penetrate the first and second line.

To accomplish this, the "Navigators" will secure free support on offer from public and private organizations, like Homeland Security, state governments, and companies like Google and Cloudflare. They will also work with outside vendors who provide much of the elections infrastructure and support to local officials. Third, they will build a culture of security that can adapt to evolving threats through training and constant re-assessment.

Voters should feel confident that we have resilient systems, with paper ballots and good audits almost everywhere. But voters should also understand that without continued investment in people and products the possibility of a successful attack increases. As does the likelihood that campaigns may cultivate cynicism about the integrity of our elections for their own purposes. Democracy is not perfect. As Churchill said, it is the worst form of government except for all the others. We need to protect it. We will regret it if our democracy is damaged because we looked away at a critical moment.

Thank you, Chairman Blunt and Ranking Member Klobuchar as well as all members. It is an honor to be here. I am reminded as an election administrator that when we certify results we are an essential part of the process that bestows not just power, but legitimacy. And that legitimacy attaches because of the essential American belief that our elections reflect a trusted and true accounting of each election. I speak to you today in support of efforts to ensure that legitimacy remains the key virtue in our elections.

My name is Noah Praetz. I am director of Elections in Cook County Illinois. I work for Cook County Clerk David Orr. Over the past 18 years, under Clerk Orr's leadership our office has tried to lead on technology and security - using applied forensics in elections; creating widely circulated cyber-security checklists in advance of the 2016 elections; and publishing the first white paper written by election officials in the wake of the 2016 attacks. Recently, I helped the Center for Internet Security (CIS) adapt their digital security expertise to the unique context of elections and also spent a little time talking to the Defending Digital Democracy program at Harvard's Belfer Center (DDD). As co-chair of the Government Coordinating Council (GCC) that the Department of Homeland Security created to help address election security, I have worked with federal, state and local leaders in elections, technology, intelligence and law enforcement.

In the past 10 months I have on two occasions testified before the United States Election Assistance Commission (EAC) and on two occasions I have testified before Illinois legislative committees. I have presented before the numerous meetings of election officials from Illinois and from around the country. Every time, I strive to deliver the same message:

- The threats to election infrastructure are real.
- Elections are largely run and secured locally, so security efforts need to be concentrated locally.

As election officials, we must accept the conclusion of the intelligence community - our elections were attacked. And while enemy hostile probes of our news and influence systems appear to have been more successful than those on election administration, we have to expect the attacks will evolve. We, as election administrators, must defend our section of the line – by securing all elements of our voting infrastructure.

Cyber-Security – One More Sword to Juggle

Prior to 2000, election administrators served mostly as wedding planners, making sure the right list of people came together in the right place with the right stuff. After *Bush v. Gore*, the Help America Vote Act (HAVA) heralded in new era of voting technology, and we became legal compliance and IT managers. We've been working to protect digital technology since then. But the 2016 election showed irrefutably that sophisticated attacks are to be expected and that we must also be cyber-security managers

Foreign governments, foreign non-state actors, and domestic troublemakers have the capacity and desire to corrode the essential public belief that our election outcomes are true and reliable. To very different degrees, this threat applies to both preliminary returns announced on

election night and to official, final results. Beyond corrupting election results, the threat also reaches the large variety of systems used to run seamless elections.

Therefore, the new security mantra, or security framework, for local election officials must be "defend, detect, recover."

Security isn't just about defense. Perfect defense is difficult or even impossible. I could cite a list of our best companies and government entities that have been breached despite significant defensive investments. Instead, the challenge of security is to ensure no attack exceeds our resilience–our ability to detect and recover–whether that requires restoring lost data or even recounting ballots - to establish election results that are trusted and true.

Because state laws vary, local election officials confront a different security matrix in each state, affecting their ability to defend, detect and/or recover. States with great audits (detection) and paper ballots (recovery) are much more resilient by definition; and the burden of defending their voting system perfectly is consequently much lower. On the other hand, states without great audits and without paper ballots place the unenviable burden of perfect defense on their local election administrators.

In 2017, Cook County Clerk David Orr and I published a White Paper called "2020 Vision: Election Security in the Age of Committed Foreign Threats." It is included at the back of this testimony. But I want to acknowledge that different bodies of this congress have already taken action that broadly agrees with our vision and I commend that work.

Elections are Secured Locally

I have tremendous appreciation and respect for state election officials and their responsibilities and efforts. They are often the mouthpiece of our institution and responsible for managing the regulatory framework. For the past 15 years many have also managed their state's voter registration systems. In some states they take a far more active role in protecting other parts of the infrastructure. And it was states that were the named targets in 2016. But let there be no mistake - local election officials are on the front lines of this new battle field: 108 in Illinois and over 8,000 nationally. So by and large, local election officials secure the nation's election infrastructure. Locals install, store, monitor, test, deploy, run and audit the voting machines and software. Locals install, store, monitor, test, deploy, run and audit the electronic pollbooks. It is locals who manage warehouses, informational websites, voter databases, polling places, GIS Systems, results reporting systems, military voting systems, command centers and the myriad digital services we rely upon in modern American elections. It is a local job to defend these systems, to institute controls that would detect breach, and to deploy mitigation strategies that can guarantee election processes and results that are trusted and true. It is there job to ensure recovery.

Most of us are county officers, and we are facing down powerful, shadowy adversaries, like Andy of Mayberry sent to repel an invading army. We need advice, support, and resources – first, for better technology and routine hand counted audits which can give additional confidence that digital results are accurate. Second, and most critically today, we have a pressing need for top-notch personnel with the skills to navigate the current cyber battlefield. Our country's local

election officials need direct human support as we work to defend ourselves against the onslaught of digital threats we've been warned about.

Cook County Efforts

Since the summer of 2016 we have stepped up our efforts to protect ourselves and to protect the broader ecosystem.

We have introduced additional hand-counted audits to our state-mandated five percent machine re-tabulation. And we are pushing state legislation to add additional audits to election results – in the form of Risk Limiting Audits.

We have done a complete mapping of all our systems and conducted a point analysis of potential vulnerabilities. We have documented all defensive measures employed and created a list of those we hope to employ going forward. We also documented all methods of detecting breach, as well as those we hope to employ in the future. Finally, we are developing our recovery plans for any breach at any point on any system. Before November of this year, we will practice every recovery method.

We are finalizing the procurement of new election equipment that will be easier to defend and will make detection and recovery significantly easier.

We introduced state legislation to help local election officials bring in more expertise and cyber monitoring capability.

We worked to create a communication structure in Illinois with federal, state and local cyber experts, technology experts, law enforcement officials and election officials.

We teamed with our neighbors at the Chicago Board of Elections to hire an election infrastructure and information security officer.

We have worked with MS-ISAC to get rapid intelligence on vulnerabilities and specific threat information to our networks. And we have pushed our colleagues around the state to join it and the elections ISAC. Additionally, we have gotten threat briefings from DHS and FBI.

We worked with DHS to conduct cyber scans of our websites - and to run a full risk and vulnerability assessment. And let me say that I am glad the folks working for homeland security are on our team. I firmly believe if every election official, state or local, undertook a similar effort, there would be a deafening roar from my colleagues for more resources to procure modern technology and institute modern controls.

We worked with the folks at DEFCON on some of their activities related to training election officials on the defense of networks.

I co-chair the newly created Government Coordinating Council (GCC) set up with DHS to help drive federal policy and resource allocation. I sit alongside the Chairman of the Election

Assistance Commission (EAC), the President of the National Association of Secretaries of State (NASS), the President of the National Association of State Election Directors (NASED), and from DHS Deputy Assistant Secretary, Infrastructure Protection, National Protection and Programs Directorate (NPPD). In that roll I have tried to continually push for the advancement of local official's concerns.

In all of these efforts we have learned that coordinating efforts is critical to our individual and ecosystem success.

Coordinated Efforts

There has been a tremendous amount of attention on the states, and their relationship to the federal government and it's great to see that relationship mending and great information starting to be shared between the two groups. On the GCC we have worked hard to refine a plan for securing our sector as well as protocols for sharing information throughout the ecosystem. We are working with the private sector vendor community to ensure we have a common approach to protecting the sector.

Federal government agencies now know how to communicate to the state level election professionals and vice versa. What remains unfulfilled is the assurance that the information can get all the way down to the local level and that the locals are prepared to digest the information and take necessary action.

It is time to ensure that the successful effort to normalize relations with state officials be duplicated with local election officials. Like an iceberg, the mass, and indeed most of the risks to the nation's election infrastructure, lies below the surface. And its security lies in the hands of women and men who run elections at the local level.

Given concerns with federalism, the most likely path for successfully fortifying local election officials is through state government and state election officials. But it's important that they envision their job as helping ensure locals are resourced appropriately and meeting important security metrics. I have no doubt that our state officials are up for the challenge and I look forward to assisting our industry mature in this direction quickly.

Increased Stable Investment & Short Term Spending

We look to our state and federal funders and regulators to fortify us on this battlefield. Given the costs of regular technology refreshes and support for human resources with cyber capacity, the needed investment is very large, on the order of HAVA 2.0. We need a signal that we can invest now for security and not squirrel away recent money for some future episode.

Nevertheless, the current investment is greatly appreciated. Congress just released $380 million to combat the election cyber security threat. And that is an important start. It may be necessary to invest that much annually. Meanwhile, Americans justly concerned about the costs need confidence this money will be spent well. In my mind there are two top priorities. First,

a handful of states and counties still have paperless voting systems. These must be replaced as soon as possible.

Second, everywhere, we must improve the security capacities of local election offices. Most are run by a just handful of incredibly dedicated and hardworking heroes. But a handful of people making critical security decisions are outmatched against the threats we've been warned of.

In a local newspaper we called for a brigade of digital defenders to be deployed to serve election offices around Illinois and the nation, starting now and working through the 2020 presidential election and beyond. Recently, the Government Coordinating Council, comprised of the leadership of America's election organizations, suggested a similar construct, suggesting that states employ "cyber navigators" to help fortify local election officials.

Illinois Approach

In Illinois we formulated a loose security group consisting of representatives of Homeland Security, FBI, the Illinois State Police and their Cyber Team, Illinois Information Security Office, the leadership of the local election official associations, and the State Board of Elections. Originally our some of local officials and the State Board of Elections had desired to pass through the HAVA funds to the local election officials based largely upon voting age population. But as our group and state legislators digested the cyber security problem, we recognized that such a distribution would not be effective in fortifying most of the locals. First, regardless of the number of voters served, all 108 election officials had nearly identical cyber footprint, in that they had the same number of networked-attached digitally exposed systems. Second, the larger offices already had some capacity to tackle this problem – whereas the smaller offices are squeezed so tightly they can barely comply with the current requirements, let alone secure the entire elections threat surface area.

After the GCC issued guidance suggesting "Cyber Navigators", the state legislature mandated that at least one-half of the HAVA funds just released be expended on a "Cyber Navigator" program to be administered by the State Board of Elections. The State Board is likely to get help fulfilling this mandate from other organizations with cyber expertise. By and large, local election officials supported the bill. And our state board is eminently capable of fulfilling the mandate.

These "Navigators" need to accomplish three vital goals. First, they should work to institute the election security framework – defend, detect, recover. They can help improve defenses within election offices, following the specific recommendations of CIS. We believe they'll quickly bring up the floor of the elections security ecosystem. Appropriately supported, we can see massive improvement very quickly. There is low hanging fruit, but even low hanging fruit needs to be plucked. They'll also work to support locals' efforts at instituting detection techniques and recovery plans. Second, the "Navigators" will do the work necessary to secure the free support being offered by public and private organizations, like the Department of Homeland Security, state resources, Google and Cloudflare, or the Elections Information Sharing & Analysis Center; they will also work with the outside vendors who provide much of the

elections infrastructure and support to local officials. More importantly, they will help build a culture of security that adapts to the evolving threats we face through training and constant assessment efforts. Illinois' 108 local election offices will mature quickly with this reinforcement. As specific mitigations and upgrades are identified by Navigators, the State Board should be positioned to quickly provide that investment.

It is expected that the State Board of Elections will take some small portion of the remainder of the HAVA funds to support their own infrastructure, naturally, since they manage and maintain the statewide voter database. Everything else shall be distributed to the local election officials to invest as they see fit, subject to the guidelines. I'll note that our legislature sought to compel participation in the Navigator program by making receipt of future grants contingent upon local official participation.

In Illinois, we recognized that this is inherently a local problem. But we also recognize that locals cannot solve this problem themselves. This coordinated, managed approach assures appropriate assessment and remediation efforts can be efficiently implemented. We are utilizing existing expertise from other areas of federal, state and local government as force multipliers. And we are excited that our State Board of Elections is taking on this new mandate and moving quickly to implement it.

This massive reinforcement effort can be accomplished here and nationwide. And it can be done now. It will require the states to cut through the red-tape that can delay action. This may mean relying on existing contracts, or even emergency procurements. But states must do whatever they need to do to get the army of "Navigators" on the ground this summer. After all, the danger is not hypothetical. We're bracing against the renewed attacks we've been told to expect.

Supporting a Resilient Public

One job of an election administrator is to conduct elections so that losing candidates accept the fact that they lost fairly. Anything that hinders our ability to do that decreases confidence in the system. And undermines our ability to bestow legitimacy – not just victory.

Election officials deploy a variety of networked connected digital services, such as voter registration systems, and unofficial election results displays. Each of these is a ripe target for our adversaries. A successful attack against those services may not change a single vote, but could still damage public confidence. This is particularly true in a time of great public suspicion, exacerbated by a disappointing proliferation of gracelessness and grandstanding.

Our public confidence is already weaker than it should be. Vacillating voting rights rules, no matter how marginal the effect, are disconcerting to many people, naturally suspect given our history. Additionally, some media, activist groups and politicians have acted in ways that ultimately prey on Americans' insecurities about their most cherished institution, either through wildly outlandish claims of fraud, or through claims of suppression that are sometimes exaggerated. Such actions do hinder our ability to bestow not just victory, but legitimacy. We must be very careful to calculate not just the relative effects on power that election rule changes

can have, but also the relative effects on legitimacy. Or put another way – will losers be more or less likely to accept that they lost fairly.

Some losing candidates are already apt to call their defeats into doubt. A new digital breach - no matter how far removed from the vote counting system - could turn sore losers to cynicism, disbelief, even revolt. That's the reaction the enemies of the United States want.

In fact, in the face of direct targeting of a state or local election office it is very possible that there will be some service disruptions – most likely to the network connected digital services like election results websites.

The bottom line is we can't eliminate every chance of breach, but we can make sure that successful attacks rare. And we can provide assurances that we are prepared to recover quickly when they happen. We can do this with support at the local level. I support federal efforts like the Secure Elections Act. While I would always advocate for more local participation, in the current environment, doing something imperfect now is greatly superior to doing something perfect at some point in the future.

As Americans, we get to choose how we want to respond to potential disruptions. The damage of a foreign attack on our elections infrastructure will be greatly diminished if the targeted institution is also being supported internally with respect.

Thank you for the opportunity to appear today. I look forward to your questions.

White Paper

2020 Vision: Election Security in the Age of Committed Foreign Threats

Sponsored by: Cook County Clerk David Orr

Authored by: Noah Praetz, Director of Elections

December 2017

The entire national security establishment admonishes that threats to our election infrastructure are real. Foreign governments, foreign non-state actors, and domestic troublemakers have the capacity and desire to corrode the essential public belief that our election outcomes are true and reliable. To very different degrees this threat applies to both preliminary returns announced on election night and to official, final results.

Beyond results, the threat applies to the large variety of systems used to run seamless elections. These include electronic and paper pollbooks; voter registration and election management systems; websites with voter tools and public information; and a variety of other subsystems such as: GIS, ballot printing system, mail ballot preparation and processing system and a variety of essential election support systems like election day control centers.

Local election officials - nearly 9,000 of them in the country - are the shock troops on this new battlefield. They desperately need resources, including federal government resources.

Policymakers and funders must act now to ensure election security

The new security mantra for local election official's is "defend, detect, recover."

Perfect defense is difficult or even impossible. Instead the challenge of security is to ensure no attack exceeds our resilience–our ability to detect and recover–whether that means restoring lost data or even recounting ballots to establish election results that are trusted and true.

Each state has a varying security matrix to operate in; their mix of ability to defend, detect and recover. States with great audits (detect) and paper ballots (recover) are much more resilient by definition; and the burden of defending their voting system is consequently much lower. On the other hand, states without good audits and without paper ballots place the unenviable burden of perfect defense on their election administrators.

Below is a challenging, comprehensive, yet achievable list of actions to protect the integrity of these multiple systems. Make no mistake, this will be a painful and expensive undertaking. But the protection of our foundational institution requires this sacrifice.

Responsibilities of Policymakers and Funders:

Defend

Increase the defensive capacity of local and state election officials by:

1. Supporting a digital network for all local election officials that will facilitate rapid sharing of threats and incidents, as well as supporting increased training and resiliency;
2. Financing an Election Infrastructure and Information Security Officer (EIISO) (or consultant) servicing every local and state election official in the country;
3. Ensuring that threat and incident information known to Government is shared appropriately throughout the election ecosystem.

Detect

Increase the catastrophic breach detection capacity by incentivizing:

1. The use of modern public audits of all elections;
2. The use of modern voting technology that captures a digital image of each ballot that can be tied to the original ballot and the cast ballot record;
3. The use of monitoring sensors on the networks of all willing election officials.

Recover

Eliminate even the most remote possibility of an undetectable catastrophic breach by replacing all paperless voting systems that currently serve nearly 20 percent of the country.

Release election officials from their burden of being perfect every single time!

Potential Approach for Election Officials and Their Election Infrastructure and Information Security Officer:

Defend

- Get experts into the office. Engage outside cyber security resources & professionals. No election offices can handle this problem on their own. Inside most elections offices, there simply is not the complete capacity to accept the threat, assess the vulnerability, digest recommendations, manage mitigations and perfect recovery.
    - Utilize as many free local, state, and federal (DHS, CIS and MS-ISAC) tools as possible,
        - If government resources are unavailable, or underwhelming, hire private firms or partner with academic institutions.
    - Collaborate with resources inside local, state and federal government because we are not alone in facing this type of threat include the fusion centers.

- Bring in outside resources to partner with information technology and information security teams, with a focus solely on election security.
    - The reality is that most election officials share their internal information technology and security resources with every other county office engaged in critical activities, such as health and public safety. It can be nearly impossible to get the attention necessary for election security unless it is the primary focus of those resources.

- Understand and limit the threat surface area; or all possible points of vulnerability for malicious attack.
    - Inventory all election related systems: e.g. voting machine and vote counting system; e-pollbook system; voter registration / election management system; mail ballot delivery and processing system; and online-systems such-as voter registration, mail ballot request tools, voter information lookup;
    - Map how systems work and data flows, and mark every single point of vulnerability;
    - Limit the threat surface area by making policy decisions that reduce points of vulnerability wherever possible (this is about managing risk, not eliminating it.)

- Employ defense tactics and policies for each system – online or not;
    - Implement the Center for Internet Security's top 20 cyber controls. Do the top 5 first. These include:

        1. Inventory of Authorized and Unauthorized Devices
        2. Inventory of Authorized and Unauthorized Software
        3. Secure Configurations for Hardware and Software
        4. Continuous Vulnerability Assessment and Remediation
        5. Controlled Use of Administrative Privileges
        6. Maintenance, Monitoring, and Analysis of Audit Logs
        7. Email and Web Browser Protections
        8. Malware Defenses
        9. Limitation and Control of Network Ports
        10. Data Recovery Capability
        11. Secure Configurations for Network Devices
        12. Boundary Defense

13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control
17. Security Skills Assessment and Appropriate Training to Fill Gaps
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

- Employ election system-specific defense and detection tactics across specific systems;
    - These can include all the hardening options that systems may have, such as locks, seals, chain of custody, advanced authentication, etc.

Detect

- For each vulnerability point identified in the mapping process, consider a method of detecting whether something anomalous has happened; or brain storm the first place such an intrusion might be detectable.
- Validate everything; every available log should be checked including: seals, time sheets, cameras, swipe cards, login data, registration statistics, etc.
    - Behavioral analysis tools and procedures can and will point out what is going on. For example, voter registration follows a natural pattern year over year. Identifying the pattern and watching for anomalous behavior works.
- Use forensics when possible.
    - A forensics analysis of the software system employed can offer a high level of confidence that it is operating as certified. This is particularly true in the voting system environment. Comparing snapshots of deployed software with a clean reference copy during a live election is a powerful verification technique.
- Conduct public audits of the election results that allow for a visual comparison of the cast ballot record with the ballot itself.
    - Be transparent and brace for public scrutiny.
    - Crowdsourcing the election brings the greatest confidence, but also the greatest public scrutiny. "Sausage making" will be on full display. Consider publishing ballot images scrubbed of identifying marks. In the short run this

can create volatility, and people may scrutinize the office and the software used, but ultimately the confidence levels will be increased.

- Work to investigate audit styles that bring the highest level of confidence to the most stakeholders. Consider the use of sophisticated yet efficient testing algorithms, such as risk limiting audits.

Recover

- For each vulnerability point, assume a successful breach and determine how to recover.
- Where possible, make policy decisions and investments that yield the clearest path to recovery.
    - For example, on electronic voting machines: after removing paperless systems consider that, ballot marking devices are better than machines with paper audit trails. Digital scanning devices that create images of ballots are better than scanning devices that don't.
- Build in redundancy that doesn't rely on technology.
    - For example, paper pollbooks backup electronic pollbooks. Emergency paper ballots backup corrupted (or just malfunctioning) touch-screen or ballot marking devices.
- Practice recovery with professional staff, advisors and vendors by running drills and exercises. Theory is only theory. Practice makes it real.

Local election officials need support

It must be underscored – local election officials are the front-line troops in this battle. Those who control Federal, State, and local spending must provide local election officials with resources to do their job in this environment. Those who drive state election policies must make choices to fortify local officials for their new cyber mission.

Election officials are serving valiantly and professionally. They are talented and capable. They are holding the line. But they are operating with limited resources under sometimes unfair burdens placed upon them by policy makers in their respective states. Like good servants, they will say they can continue to hold the line. And they'll mean it.

But they need to be asked to hold a reasonable line. And holding a line that requires perfect defense every time is not reasonable.

It is impossible to defend against every conceivable attack. But if we detect breaches and recover from them quickly, we will survive any incident.

And so will faith in our democracy.

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.

SECRETARY OF STATE
STATE OF LOUISIANA

R. KYLE ARDOIN
SECRETARY OF STATE

P.O. BOX 91125
BATON ROUGE, LA 70821-9125
225.922.2880

June 19, 2018

Senator Roy Blunt
Chairman
Senate Rules & Administration Committee
Washington, DC

Sen. Amy Klobuchar
Ranking Member

Senators Blunt and Klobuchar,

It has come to my attention that the Senate Rules Committee will be holding a hearing on elections preparedness for 2018 and the state's work with the Department of Homeland Security (DHS) on cybersecurity. I understand that Senator Amy Klobuchar (D-MN) has co-authored a bill with Senator Lankford (R-OK) which raises potential issues that I want to be on record.

First, the proposed legislation renames the U.S. Election Assistance Commission's Technical Guidelines Development Committee (currently responsible for drafting the EAC's Voluntary Voting System Guidelines) to the Technical Advisory Board. The makeup of the Board would consist of four members, one of which is selected by the National Association of Secretaries of State and must be a State election information technology director. The fact that the Board would merely have one voice from within a state is simply unacceptable. Even though information technology directors play an important role in modern elections, they do not represent the "big picture." The State's Chief Elections Officer is the party responsible for all aspects of that State's elections, not just those related to IT, and will be the one to implement the policies and procedures adopted by this advisory group.

The legislation does not alter the committee's present duties of creating voluntary guidelines for voting systems, but it does add the duties of drafting election security and audit guidelines. Why are the audit and election security guidelines not also voluntary? There is no one-size-fits-all approach to elections. What works in one state may not work in another. I believe that voluntary, best-practices guidelines for elections security and auditing would be a much better approach for all concerned. States should be allowed the opportunity to determine their own audit guidelines.

Furthermore, the proposed Audit Guidelines, Sec. 4(b)(2), restricts the types of voting machines a state can use, which is something the authors originally said they would not do. It also seems to fall in line with papers recently discovered that proved DHS was/is looking at determining mandated voting systems as designed by DHS.

The required auditing provisions also necessitate that election agencies count *by hand* a random sample of the marked ballots prior to the winning candidate being sworn into office. Because of the way Louisiana's congressional elections are structured, with the general election held in December (if required), this could create a situation delaying Louisiana's congressional members from taking office by the required timeline of other members, resulting in their being seated later than the scheduled January deadline.

Moreover, in the case of a very close race for US Senate, as occurred in 1996 (only 5,000 votes separated the two candidates), it would be impossible for Louisiana to hand count enough ballots to "establish high statistical confidence in the election result" before the winning candidate is sworn into office in January.

I am positive that it is not the intent of this Committee to impose unfair burdens on the way that states conduct their elections, and I am happy to communicate with you further if you need clarification or testimony.

Regards,

R. Kyle Ardoin
Louisiana Secretary of State

Senate Committee on Rules and Administration
Election Security Preparations: A State and Local Perspective
June 20, 2018
Questions for the record
Honorable John R. Ashcroft

Senator Wicker

1) As secretaries of state, you know more about the challenges facing your state than anyone else. We in Congress want to make sure your Federal partners are providing you with every possible resource to help you maintain the integrity of your data and election infrastructure. What areas do you feel Federal assistance is most needed and how would you like to see those resources distributed? **Mr. Ashcroft did not respond. When received, answer will be retained in committee files.**

2) FOLLOW-UP: Some of my colleagues have introduced a bill that addresses some of the problems we are facing in protecting our election. Do you feel legislative action is necessary to address this issue, and do you think the Secure Elections Act is an adequate measure to help you face the coming elections? **Mr. Ashcroft did not respond. When received, answer will be retained in committee files.**

Senator Feinstein

1) What steps have you taken to increase the flow of information between your agency and the Department of Homeland Security (DHS)? **Mr. Ashcroft did not respond. When received, answer will be retained in committee files.**

   Specifically, please provide the following information:
   a. Have you requested information from DHS about specific election vulnerabilities in your state or jurisdiction, including vulnerabilities in election infrastructure? **Mr. Ashcroft did not respond. When received, answer will be retained in committee files.**

   b. Have you shared information with DHS about specific election vulnerabilities that you have identified in your state or jurisdiction? **Mr. Ashcroft did not respond. When received, answer will be retained in committee files.**

   c. Has DHS conducted a risk-and-vulnerability assessment of your state or any voting jurisdiction therein? If not, have you requested DHS to conduct such an assessment? **Mr. Ashcroft did not respond. When received, answer will be retained in committee files.**

2) The Consolidated Appropriations Act of 2018 included $380 million in funding available to be distributed to the states as HAVA Election Security Fund grants.

   a. To date, has your state requested any funding under the HAVA Election Security Fund grant program? **Mr. Ashcroft did not respond. When received, answer will be retained in committee files.**

   b. If so, what improvements to election infrastructure and security have you undertaken with that funding? **Mr. Ashcroft did not respond. When received, answer will be retained in committee files.**

c. If not, why have you not yet requested funding, and when do you plan to make a formal request of the Election Assistance Commission (EAC) for such funding? **Mr. Ashcroft did not respond. When received, answer will be retained in committee files.**

d. If you have not yet undertaken any improvements, how do you intend to use the funds allocated pursuant to the Consolidated Appropriations Act of 2018? **Mr. Ashcroft did not respond. When received, answer will be retained in committee files.**

e. How much additional funding does your state need to upgrade its election infrastructure? **Mr. Ashcroft did not respond. When received, answer will be retained in committee files.**

3) At the June 20 hearing before the Committee on Rules and Administration, you stated that "the evidence indicates that voter fraud is an exponentially greater threat than the hacking of our elections."

a. On what basis have you reached the conclusion that "the evidence indicates that voter fraud is an exponentially greater threat than the hacking of our elections"? **Mr. Ashcroft did not respond. When received, answer will be retained in committee files.**

b. What evidence supports your claim that "voter fraud is an exponentially greater threat than the hacking of our elections?" **Mr. Ashcroft did not respond. When received, answer will be retained in committee files.**

4) What evidence do you have of voter fraud in Missouri? Please detail incidences of alleged voter fraud, whether each was investigated and/or prosecuted, and what the outcome was. Please also provide any other evidence regarding voter fraud that informed your statement before the Committee. **Mr. Ashcroft did not respond. When received, answer will be retained in committee files.**

5) Please explain the importance in terms of selection security and integrity of using two-factor authentication for state voter registration databases. **Mr. Ashcroft did not respond. When received, answer will be retained in committee files.**

6) Please explain the importance in terms of election security and integrity of using voter-verified paper ballots. **Mr. Ashcroft did not respond. When received, answer will be retained in committee files.**

7) Please explain the importance in terms of election security and integrity of conducting post-election audits. **Mr. Ashcroft did not respond. When received, answer will be retained in committee files.**

8) What steps have you taken to ensure that all eligible voters are able to register successfully and to cast their votes? Specifically, please address the following:

a. Voter registration efforts. **Mr. Ashcroft did not respond. When received, answer will be retained in committee files.**

b. Accessibility issues for voters with disabilities. **Mr. Ashcroft did not respond. When received, answer will be retained in committee files.**

c. Early voting. **Mr. Ashcroft did not respond. When received, answer will be retained in committee files.**

d. Provisional ballots. **Mr. Ashcroft did not respond. When received, answer will be retained in committee files.**

e. Compliance with Missouri's voter ID law. **Mr. Ashcroft did not respond. When received, answer will be retained in committee files.**

Senator Warner

1) Provisions that address information sharing such as the Secure Elections Act would improve sharing of threat information from federal intelligence agencies with appropriately cleared state and local election officials. However, information sharing is no cure-all, as there have been instances when state officials have misinterpreted relevant Indicators of Compromise in shared threat Intel reports, leading to confusion and potential misattribution. In addition, state officials have described the difficulty of prioritizing threats and keeping up with the vast amounts of information that is shared with them.

   Could you describe how states and local officials are building the needed capabilities to intake, analyze, and operationalize threat information? **Mr. Ashcroft did not respond. When received, answer will be retained in committee files.**

2) In the FY 2018 omnibus bill that passed this spring, $380 million in grant money was made available for states to help improve their election infrastructure. **Mr. Ashcroft did not respond. When received, answer will be retained in committee files.**

   Do you believe that election assistance funds should be tied to any particular actions on the part of states, or should they be spent as states see fit? **Mr. Ashcroft did not respond. When received, answer will be retained in committee files.**

   However, it is difficult – even for large enterprises – to choose products and services that best meet their needs.

   What resources do state election officials currently have to evaluate cybersecurity products and service vendors? **Mr. Ashcroft did not respond. When received, answer will be retained in committee files.**

   Should the Department of Homeland Security or the Election Assistance Commission provide a clearinghouse of information, which includes vetting of vendors? Are the 'cyber navigators' and cyber liaisons appropriately serving a similar function? **Mr. Ashcroft did not respond. When received, answer will be retained in committee files.**

3) In May 2018, the Senate Intelligence Committee released its first Unclassified Russia Report, which included recommendations on election security. In the report, it was found that DHS was not well-positioned to provide effective support to states confronting a hostile nation-state cyber actor. While early interactions between state election officials and DHS were strained, DHS has proven to have made progress in recent months. For one, DHS is now engaging more with state election officials, including providing necessary security clearances for these officials to ensure effective information sharing.

   How would you characterize states' engagement with DHS since 2016 – has it improved? Can you describe improvements in information sharing and the sharing of threat information? **Mr. Ashcroft did not respond. When received, answer will be retained in committee files.**

Do your states' key election officials have security clearances so that you may discuss potential threats in a classified setting? **Mr. Ashcroft did not respond. When received, answer will be retained in committee files.**

Do you believe that states should abide by any minimum standards when it comes to election security? **Mr. Ashcroft did not respond. When received, answer will be retained in committee files.**

Senate Committee on Rules and Administration
Election Security Preparations: A State and Local Perspective
June 20, 2018
Questions for the record
Honorable Jim Condos

Senator Wicker

1) As secretaries of state, you know more about the challenges facing your state than anyone else. We in Congress want to make sure your Federal partners are providing you with every possible resource to help you maintain the integrity of your data and election infrastructure. What areas do you feel Federal assistance is most needed and how would you like to see those resources distributed?

Speaking from my perspective as National Association of Secretaries of State (NASS) President, the US Department of Homeland Security (DHS) has been a very valuable resource. They have been providing direct assistance via some of their services including cyber hygiene scans, risk and vulnerability testing, hunt programs, phishing assessments and virtual tabletop exercises. They also coordinated and assisted with the establishment of the Elections Infrastructure Government Coordinating Council (EIS-GCC) with state and local election officials. The EIS-GCC has approved our Sector Specific Plan and Communications Protocols on threat information sharing and incident response plans. They have also funded the establishment of a separate Elections Information Sharing and Analysis Center (EI-ISAC) so that state and local election officials can receive election-specific indicators and Albert monitors, which track network traffic and alert us to potential problems.

The US Election Assistance Commission (EAC) and the National Institute for Standards and Technology (NIST) are vital to the work of developing Voluntary Voting System Guidelines (VVSG) and developing testing protocols against the VVSG. They are also responsible for certifying the laboratories that test voting equipment.

The EAC has also been extremely helpful in disbursing the recent election funding of $380 million approved in the 2018 Omnibus Appropriations Act. They established the guidelines quickly and shared that information with states so we could access that money as soon as possible.

Speaking individually as Vermont's Secretary of State, it is my belief that the EAC should be restored to a full complement of Commissioners, with the staffing and resources necessary to carry out their charge of best assisting states with election administration.

Most importantly, from my individual perspective, states need ongoing, dedicated funding to ensure that we have the resource support necessary to best do our jobs protecting the integrity of our elections now and into the future. Federal assistance is most critical to address

the lack of funding at the state-level for the necessary replacement of voting systems – particularly replacing any voting systems that do not use a voter-marked paper ballot with those that do. Equally critical is purchase of necessary cybersecurity upgrades for existing election management software. Provision of ongoing federal funding for election security is the most important form of federal assistance. To borrow a quote from my colleague Secretary Simon of Minnesota, "cybersecurity is like a race without a finish line – it never ends." Lump-sum funding allocations every 10 or so years is certainly helpful, but in order to address ongoing security needs in a sustainable way states need regular, ongoing funding. Ongoing investment could also help curtail future large expense needs to address emergency equipment replacement scenarios due to aging infrastructure.

FOLLOW-UP: Some of my colleagues have introduced a bill that addresses some of the problems we are facing in protecting our election. Do you feel legislative action is necessary to address this issue, and do you think the Secure Elections Act is an adequate measure to help you face the coming elections?

NASS does not have a position on the Secure Elections Act (SEA).

Personally I have been, and remain, a strong supporter of the SEA. While there were a few areas of concern I had with the bill, namely overly prescriptive audit language, and a lack of funding for states to carry out the mandates of the bill, I would like to see a bill which addresses these concerns pass.

And personally, I believe best practices would include paper ballots for all votes, and postgeneral election audits.

NOTE: It's important to note that any bill passed now, or even a few months ago, will not have an impact on the 2018 elections. Every state has different procurement guidelines, some of which require legislative approval. Responsible procurement should also include a comprehensive business analysis which takes time. At this point, we need to look ahead to 2020 with any new legislation that is passed, including the SEA.

The most important area the SEA can address is funding for states to implement any new mandates imposed including funding for the EAC.

Senator Feinstein

1) What steps have you taken to increase the flow of information between your agency and the Department of Homeland Security (DHS)?

We receive weekly updates from the Elections Infrastructure Information Sharing Analysis Center (EI-ISAC). We have met with local DHS officials and will continue to do so as needed, in addition to attending all DHS related events through NASS and the National Association of

State Elections Directors (NASED). We also receive DHS notifications through NASS/NASED. We have built relationships and established clear communication channels, in both directions, if we need to communicate with DHS on what we're seeing on a state level, and so that DHS officials can communicate information to us locally as needed. I have received my secret clearance in case the need arises for me to be briefed on classified intelligence information.

Specifically, please provide the following information:

a. Have you requested information from DHS about specific election vulnerabilities in your state or jurisdiction, including vulnerabilities in election infrastructure?

We receive a form of weekly vulnerability testing of our system from DHS called a cyber hygiene scan. Our cyber risk and vulnerability assessments were completed by a thirdparty independent contractor via penetration testing in May this year. There have not been any vulnerabilities identified by DHS that have been communicated to us. I continue to participate in monthly meetings with DHS and have not been informed of any Vermont specific vulnerabilities. We have clearly established channels of communication to and from DHS should the need arise to communicate about risks or threats detected.

b. Have you shared information with DHS about specific election vulnerabilities that you have identified in your state or jurisdiction?

We have not. Our most recent risk assessment and penetration testing report showed only one vulnerability, which was multiple points of entry to our election system. The recommendation by our contractor to address this vulnerability was implementation of two-factor authentication, which we already had in process, and which is now in full implementation.

c. Has DHS conducted a risk-and-vulnerability assessment of your state or any voting jurisdiction therein? If not, have you requested DHS to conduct such an assessment?

We utilize weekly cyber hygiene scans provided by DHS. This is a form of vulnerability testing. We have not requested that DHS perform a risk-and-vulnerability assessment. We had already contracted a vulnerability penetration test by a third-party security vendor. We have asked DHS for a vulnerability and penetration test but it will not occur until after the general election. We believe it is a good thing to have a different set of eyes look at our systems.

2) The Consolidated Appropriations Act of 2018 included $380 million in funding available to be distributed to the states as HAVA Election Security Fund grants.

a. To date, has your state requested any funding under the HAVA Election Security Fund grant program?

Yes. Vermont requested and has received $3 million in appropriated HAVA funds.

b. If so, what improvements to election infrastructure and security have you undertaken with that funding?
HAVA funding has allowed us to implement a new accessible voting system, complete program penetration tests, conduct cyber training for local officials, and implement twofactor authentication for any individual who has access to our election administration system.

c. If not, why have you not yet requested funding, and when do you plan to make a formal request of the Election Assistance Commission (EAC) for such funding?

N/A

d. If you have not yet undertaken any improvements, how do you intend to use the funds allocated pursuant to the Consolidated Appropriations Act of 2018?

In addition to the expenditures noted above, we intend to use these funds to replace our aging vote tabulators, hopefully by 2020, which will include physical replacement and the appropriate software installation. As detailed in our budget narrative, we have also dedicated funding to ongoing cybersecurity upgrades.

e. How much additional funding does your state need to upgrade its election infrastructure?

Due to the ongoing, evolving nature of the cyber threats to election security, there will never be a finite amount needed to adequately update our infrastructure. Elections infrastructure will need constant maintenance and upgrade in order to stay ahead of threats to it. Ongoing, sustainable annual funding is the most appropriate way to address this threat in a serious, committed manner.

3) At the June 20 hearing before the Committee on Rules and Administration, Secretary of State Ashcroft stated that "the evidence indicates that voter fraud is an exponentially greater threat than the hacking of our elections."

a. Do you agree with Secretary Ashcroft's claim that "the evidence indicates that voter fraud is an exponentially greater threat than the hacking of our elections"?

No, and I would ask Secretary Ashcroft to produce the "evidence" of voter fraud on which he bases that claim. Every reputable study I have seen has found widespread voter fraud to be practically, if not actually, non-existent. In contrast, the entire U.S. intelligence community is in agreement about the cyber threat posed to our elections by our foreign

adversaries. I couldn't disagree more with Secretary Ashcroft and urge the Senate to focus on the real, substantiated cyber threat to our democracy.

What occurred in 2016 was not meddling or interference, it was an attack on our democracy.

b. If so, on what basis have you reached that conclusion?

N/A

4) Please explain the importance in terms of election security and integrity of using two-factor authentication for state voter registration databases.

First, I am speaking individually as Vermont's Secretary of State. NASS does not, as of yet, have an official position on best practices for election security, or on individual state practices.

Two-factor authentication is universally recognized across industries as the easiest, mostimportant baseline step that can be taken to protect web-based systems from a cyber-attack. Two-factor authentication ensures that, even if a user's password is stolen, there is another layer of security beyond that that which would prevent a bad actor from accessing a given system, even though they have obtained a user's password.

5) Please explain the importance in terms of election security and integrity of using voterverified paper ballots.

Speaking as the Vermont Secretary of State, using a paper ballot ensures that, despite whatever else may happen, there is always a paper record of every voter's vote which can be counted and recounted in order to determine the actual result. It is the ultimate "fail-safe" in the case of any worst case scenario of an attack on an election. Moreover, even in the absence of an attack, use of paper ballots ensures the ability to effectively audit the results of an election and confirm the original result. We have always used a paper ballot in Vermont, and it is actually mandated in statute.

6) Please explain the importance in terms of election security and integrity of conducting postelection audits.

Post-election audits provide the opportunity to expose any irregularities in the official result and, of equal importance, provide the public confidence in the announced result. Like the use of paper ballots, effective auditing is a fundamental way to expose any irregularities or evidence of tampering while providing a method to ensure that results can be verified. Vermont began completing post-general election audits in 2006 and have continued that practice ever since. We actually strengthened our post-election audit procedure in 2012.

Senator Warner

1) Provisions that address information sharing such as the Secure Elections Act would improve sharing of threat information from federal intelligence agencies with appropriately cleared state and local election officials. However, information sharing is no cure-all, as there have been instances when state officials have misinterpreted relevant Indicators of Compromise in shared threat Intel reports, leading to confusion and potential misattribution. In addition, state officials have described the difficulty of prioritizing threats and keeping up with the vast amounts of information that is shared with them.

   Until several months ago, there was no official state-by-state contact list. So, the people who needed the information may not have received it in a timely manner. For instance, here in Vermont, the Secretary of State is independently elected and on its own IT system. We are not part of the state IT protocol. In instances like these, if information was shared with a state Chief Intelligence Officer, it thus may have been sent to the wrong area. We have developed better streams of communication in-state, and in partnership with DHS, to address this.

   Could you describe how states and local officials are building the needed capabilities to intake, analyze, and operationalize threat information?

   State and local election officials are working with DHS and the EI-ISAC to process and address threat information. Many states have also ramped up in-house cyber staff over the past year and with the new federal funding are hiring additional staff to assist locals. The EIS-GCC approved new communications protocols that address federal-state and local information sharing and we are busy testing those protocols through tabletop exercises held by individual states and through the DHS National Virtual Tabletop Exercise.

2) In the FY 2018 omnibus bill that passed this spring, $380 million in grant money was made available for states to help improve their election infrastructure.

   Do you believe that election assistance funds should be tied to any particular actions on the part of states, or should they be spent as states see fit?

   While all states share some similarities when it comes to funding elections administration, each state also has its own unique needs. The most recent round of funding was remaining unappropriated dollars from the Help America Vote Act of 2002, and thus tied to the parameters of that legislation.

   I think it is appropriate for any legislation to require that states using any federal funds going forward to replace their voting systems must replace them with systems that use a votermarked paper ballot. In Vermont, we have a paper ballot for each vote cast. It's critical any federal mandate requiring an expenditure by states be accompanied by adequate funding to meet that mandate.

It's also important for Congress to understand that each state system of election administration is different. Our decentralized system of election administration is actually one of our greatest defenses against a wide-scale attack on our elections or election systems. Specific election administration, process, or system mandates by Congress should, largely, focus on the goal or outcome to be accomplished, rather than the specific path to accomplish that outcome. For instance, while I believe requiring post-election audits is appropriate, states need language that requires them to conduct an audit with a high degree of statistical confidence, rather than language that legislates a specific procedure.

However, it is difficult – even for large enterprises – to choose products and services that best meet their needs.

What resources do state election officials currently have to evaluate cybersecurity products and service vendors?

In general I cannot answer for the states. However, I can say that many states have, through their General Services or Procurement systems, a pre cleared vendor list. This is also an area where the EAC could be beneficial.

Specifically to Vermont, I rely largely on my IT Director to evaluate cyber security products and vendors, while other larger states have whole teams or departments dedicated to this work.

Should the Department of Homeland Security or the Election Assistance Commission provide a clearinghouse of information, which includes vetting of vendors? Are the 'cyber navigators' and cyber liaisons appropriately serving a similar function?

Soon after the Omnibus funding was released, the EIS-GCC developed the Election Infrastructure Security Funding Considerations with advice and questions to consider when selecting a vendor. Both the EAC and DHS are part of the EIS-GCC. States are working with the resources available to them to assist local election officials with these issues. I'm not sure how a "vetting of vendors" happens, but I think many would welcome this.

I would support strengthening the EAC by providing it with a full complement of Commissioners (right now they cannot meet to take any action due to a lack of a quorum) and the resources to ramp up their ability to assist the states even more.

3) In May 2018, the Senate Intelligence Committee released its first Unclassified Russia Report, which included recommendations on election security. In the report, it was found that DHS was not well-positioned to provide effective support to states confronting a hostile nationstate cyber actor. While early interactions between state election officials and DHS were strained, DHS has proven to have made progress in recent months. For one, DHS is now

engaging more with state election officials, including providing necessary security clearances for these officials to ensure effective information sharing.

How would you characterize states' engagement with DHS since 2016 – has it improved? Can you describe improvements in information sharing and the sharing of threat information?

The US Department of Homeland Security (DHS) has become a very valuable resource. They would be the first to say that it was a rocky road in the beginning – but we have overcome. We communicate and work together well at this point.

They have been providing direct assistance via some of their services including cyber hygiene scans, risk and vulnerability testing, hunt programs, phishing assessments and virtual tabletop exercises. They also coordinated and assisted with the establishment of the Elections Infrastructure Government Coordinating Council (EIS-GCC) with state and local election officials. The EIS-GCC has approved our Sector Specific Plan and Communications Protocols on threat information sharing and incident response plans. They have also funded the establishment of a separate Elections Information Sharing and Analysis Center (EI-ISAC) so that state and local election officials can receive election-specific indicators and Albert monitors, which track network traffic and alert us to potential problems.

Do your states' key election officials have security clearances so that you may discuss potential threats in a classified setting?

DHS has worked diligently to expedite the clearance process for each state's chief election official, along with two additional key staff in each office. I think most have interim or final clearance. Of course, we'll have to go through this all over again in a number of offices after November, which is why some didn't go through the process at all. However, DHS has also assured us that if necessary, they can grant a one-day clearance in order to provide critical information.

Do you believe that states should abide by any minimum standards when it comes to election security?

NASS does not have an official position on this. While I personally don't object to minimum standards, it's important that those standards are accompanied by the funding necessary for states to ensure that they are meeting those standards.

Senate Committee on Rules and Administration
Election Security Preparations: A State and Local Perspective
June 20, 2018
Questions for the record
Honorable Steve Simon

Senator Wicker

1) **As secretaries of state, you know more about the challenges facing your state than anyone else. We in Congress want to make sure your Federal partners are providing you with every possible resource to help you maintain the integrity of your data and election infrastructure. What areas do you feel Federal assistance is most needed and how would you like to see those resources distributed?**

States need resources to harden our state election infrastructure and to provide resources to local election officials to do the same. While one-time money distributed to the states will assist states in addressing immediate needs, we know that ongoing funding is needed. Investing in enhanced election security is not a one-time endeavor, and requires ongoing funding. Because state election systems have become the target of nation-state actors, and because we have been told repeatedly by federal intelligence officials that these attempted attacks will likely continue into the foreseeable future, I would encourage the federal government to explore ongoing financial support to state and local elections officials.

2) **FOLLOW-UP: Some of my colleagues have introduced a bill that addresses some of the problems we are facing in protecting our election. Do you feel legislative action is necessary to address this issue, and do you think the Secure Elections Act is an adequate measure to help you face the coming elections?**

Legislative action is necessary and I support the Secure Elections Act. It recognizes the very real threat that we face. It would provide floors, not ceilings, for state action to secure elections. It would provide guidelines and best practices that reflect the very real federal interest in ensuring that all elections in all of the states are administered with care and skill. I think the latest version of the bill strikes the right balance – by ensuring state control of elections, but with reasonable and measured help from the federal government. Additionally, this bill allows for more coordination between the states and federal government, something that is needed in light of ongoing threats by foreign entities attempting to meddle in our elections.

Senator Feinstein

1) **What steps have you taken to increase the flow of information between your agency and the Department of Homeland Security (DHS)?**

The Department of Homeland Security has offered election officials around the country several resources, and my office has actively engaged with the Department to take advantage of those resources. The Department completed various assessments of Minnesota's election systems well ahead of the 2018 midterm elections, including the risk-and-vulnerability assessment. Further, my office regularly communicates with federal law enforcement and intelligence officials in both classified and unclassified settings. This relationship has helped my office tremendously when it comes to identifying and addressing cyber security needs to safeguard Minnesota's elections.

Another effort to increase the flow of information between my office and the Department of Homeland Security is the Elections Government Sector Coordinating Council (GCC), of which I am a member. The GCC was established to ensure federal information and resources reached state and local election officials. The council allows for more communication between federal, state, and local officials to secure elections and share information in a timely manner.

Specifically, please provide the following information:

a. **Have you requested information from DHS about specific election vulnerabilities in your state or jurisdiction, including vulnerabilities in election infrastructure?**

Yes, Minnesota asked for and received both a cyber-resilience and a risk-and-vulnerability assessment from the Department of Homeland Security prior to the 2018 midterm election.

b. **Have you shared information with DHS about specific election vulnerabilities that you have identified in your state or jurisdiction?**

Yes, in addition to the information shared as part of the Department of Homeland Security's cyber-resilience and risk-and-vulnerability assessments, my office has shared additional information about the security and potential vulnerabilities of the state system.

c. **Has DHS conducted a risk-and-vulnerability assessment of your state or any voting jurisdiction therein? If not, have you requested DHS to conduct such an assessment?**

Yes, Minnesota asked for and received a risk-and-vulnerability assessment from the Department of Homeland Security prior to the 2018 midterm election.

2) **The Consolidated Appropriations Act of 2018 included $380 million in funding available to be distributed to the states as HAVA Election Security Fund grants.**

a. **To date, has your state requested any funding under the HAVA Election Security Fund grant program?**

Yes, Minnesota requested our full share of $6,595,610. Minnesota state law requires that when federal money is made available to the Secretary of State, legislative approval is needed to access the funds. *See* Minn. Stat. § 5.30 (2018). I requested that the legislature authorize use of these funds. Unfortunately, the legislature chose to attach the necessary authorization language to a bill that was doomed never to be enacted. This means my office will not be able to access these funds prior to the 2018 election.

b. If so, what improvements to election infrastructure and security have you undertaken with that funding?

As indicated in my previous answer, Minnesota state law requires legislative approval to access these funds and we did not receive this appropriation during the 2018 legislative session. Because of this, we are currently unable to use these funds. The next opportunity for the legislature to approve use of these funds will be when the legislature reconvenes for the 2019 legislative session in January.

c. If not, why have you not yet requested funding, and when do you plan to make a formal request of the Election Assistance Commission (EAC) for such funding?

My office requested full funding from the Election Assistance Commission on June 7, 2018. Unfortunately, as previously mentioned, Minnesota state law requires legislative approval to access these funds and we did not receive this appropriation during the 2018 legislative session.

d. If you have not yet undertaken any improvements, how do you intend to use the funds allocated pursuant to the Consolidated Appropriations Act of 2018?

My office has identified an immediate need of approximately $1.5 million for a project to rewrite the code of the Statewide Voter Registration System (SVRS), first developed in 2003 and 2004 with the initial HAVA funds provided in Title I and Title III. This remains my highest priority, and will be a four year project requiring three additional staff to complete. The uses for the remaining 2018 HAVA funds are yet to be determined. My office has convened a working group consisting of election stakeholders statewide to address this very issue. This working group will review statewide election needs, including hardware, software, personnel, and local election officials' training for cybersecurity and accessibility. My office will then provide the state legislature with a proposal for the use of these funds (shaped by the advice of this working group) in hopes of receiving appropriation for them during the 2019 legislative session.

e. How much additional funding does your state need to upgrade its election infrastructure?

Election security is a race without a finish line. The money provided as part of the Consolidated Appropriations Act of 2018 was an excellent start and will enable Minnesota to continue to implement the recommendations given to us by federal law enforcement

and intelligence officials, and keep Minnesota on par with industry standards. Once appropriated by our state legislature, these funds will allow us to buy software and hardware to help secure and strengthen our elections and to provide resource and support to local election officials. But in order for these things to be effective, there needs to be a significant amount of resources invested in people who specialize in the IT industry, people who often times are the highest paid people in the office. My office plans to hire three additional staff members to secure and modernize our Statewide Voter Registration System, and to hire a state-level security professional that can provide resources and support to local election officials. The cost to sustain these positions will be ongoing.

In addition to staff time and resources, with each recommendation from the Department of Homeland Security that we implement, one can reasonably expect there will be ongoing annual fees for security patches, upgrades, and support.

We will continue to need federal partnership. Additional funding is needed to strengthen and extend the protections to our election security. Ongoing dedicated funds that states can use for more software, more hardware, and human expertise will be essential as technology changes and foreign adversaries become more sophisticated.

3) At the June 20 hearing before the Committee on Rules and Administration, Secretary of State Ashcroft stated that "the evidence indicates that voter fraud is an exponentially greater threat than the hacking of our elections."

a. Do you agree with Secretary Ashcroft's claim that "the evidence indicates that voter fraud is an exponentially greater threat than the hacking of our elections"?

Based on my conversations with federal law enforcement and intelligence officials, I believe that cyber security in particular is the most significant threat to the integrity of our election system.

b. If so, on what basis have you reached that conclusion?

I have come to the conclusion that cyber security in particular is the most significant threat to the integrity of our election system after numerous conversations with federal law enforcement and intelligence officials. Minnesota was identified as one of 21 states whose election systems were targeted in 2016 by people working "at the behest of the Russian government." While there was no actual intrusion in Minnesota, and my office was able to block the would-be hackers from entering our system, intelligence officials have confirmed that these agents did scan our system with the intention of doing more. I have been advised that my office, and election officials around the country, should be prepared for more sophisticated efforts to interfere electronically in our elections.

4) **Please explain the importance in terms of selection security and integrity of using two-factor authentication for state voter registration databases.**

At a time when phishing attacks are as prevalent as they are, it is important we safeguard our information as best we can, and multi-factor authentication is simply another lock on the door. This industry standard makes it more difficult for an unauthorized person or entity to gain access to a system, specifically Minnesota's Statewide Voter Registration System (SVRS), by requiring more than one method to verify a person's identity.

With hundreds of county and local election officials accessing SVRS, it is vital to the integrity of our elections that each and every person has the proper authorization to do so. Should there be any sort of phishing attack wherein the victim provides their log-in information, two-factor authentication helps ensure that the individual or entity that conducted that attack will still not have access to the millions of records within SVRS without a piece of additional information that only the authorized user has with them.

5) **Please explain the importance in terms of election security and integrity of using voter-verified paper ballots.**

I am proud that Minnesota uses paper ballots, something invulnerable to hacking. As a result of using paper ballots, there is always a paper trail to ensure the integrity of our elections.

While we do use electronics to assist in vote counting, Minnesota is not dependent on such electronics, and final vote tallies are ultimately based off paper ballots. Voters use paper ballots and when they have completed voting, the voter inserts the ballot into a tabulator which tells them that their ballot has been accepted. At the end of election night, each tabulating machine prints out a paper receipt of the vote counts for the machine. No tabulating machine is connected to the internet while voting or tabulating is taking place.

The vote count printed from the tabulating machine is checked against the number of paper ballots, and all receipts and paper ballots are retained for 22 months as prescribed in both state and federal law.

Paper ballots allow my office to conduct post-election audits of randomly selected precincts to double check that the machines counted the Election Day results accurately. This is a public process where the votes on the ballots from the randomly selected precincts are counted by hand and verified against the Election Day paper receipts generated by the tabulating machine. If the audits were to discover machine tabulating issues, the audit would escalate to include additional precincts. Since the audits were first conducted after the 2006 State General Election, there has been no escalation.

When paper ballots are paired with post-election audits, the risk to an attack on our vote tally or outcome of our election is very low, and I am confident that votes of Minnesotans will be counted accurately.

6) Please explain the importance in terms of election security and integrity of conducting post-election audits.

In order to ensure the integrity of our elections, we need to proactively check our system for potential errors, and post-election audits are one way we are able to do that. We conduct post-election audits of randomly selected precincts to verify the accuracy of the Election Day machine tabulation of Election Day results. This is a public process. If the audits were to discover machine tabulating issues, the audit would escalate to include additional precincts. Since the audits were first conducted after the 2006 State General Election, there has been no escalation. These post-election audits promote public confidence in our elections system.

As stated above, with the use of both paper ballots and post-election audits, the risk to an attack on our vote tally or outcome of our election is very low and I am confident that votes of Minnesotans will be counted accurately.

Senator Warner

1) **Provisions that address information sharing such as the Secure Elections Act would improve sharing of threat information from federal intelligence agencies with appropriately cleared state and local election officials. However, information sharing is no cure-all, as there have been instances when state officials have misinterpreted relevant Indicators of Compromise in shared threat Intel reports, leading to confusion and potential misattribution. In addition, state officials have described the difficulty of prioritizing threats and keeping up with the vast amounts of information that is shared with them.**

   Could you describe how states and local officials are building the needed capabilities to intake, analyze, and operationalize threat information?

   Communication with the Department of Homeland Security, federal law enforcement, and other intelligence officials has significantly increased since the 2016 election. They have helped us, both in person and remotely, to identify potential vulnerabilities and best practices. Two high-level staff members and I have security clearances which allow us to receive regular briefings. With these security clearances, we are able to discuss potential threats and solutions collaboratively. However, there is a real need to streamline this information, and so in October of 2017 the Elections Government Sector Coordinating Council (GCC) was established to ensure federal information and resources reached state and local election officials. The council, which I am a member of, allows for more collaboration between federal, state, and local officials to secure elections and share information in a timely manner.

   In addition to the GCC, the Multi-State Information Sharing and Analysis Center (MS-ISAC) created Election Infrastructure ISAC (EI-ISAC) to support election cybersecurity needs. Through EI-ISAC, election specific alerts are sent to state and local election officials, focusing on sector specific threat intelligence products, incident response and remediation, threat and vulnerability monitoring, cybersecurity awareness and training products and tools for implementing security best practices.

   As Secretary of State, I hope to use the 2018 HAVA Federal Election Funds to hire a staff person dedicated to working with election officials on the county and city level, providing cybersecurity training and upgrades.

2) **In the FY 2018 omnibus bill that passed this spring, $380 million in grant money was made available for states to help improve their election infrastructure.**

   Do you believe that election assistance funds should be tied to any particular actions on the part of states, or should they be spent as states see fit?

   States need to have the flexibility to use assistance funds to best fit their individual needs. Every state is different, and each state is at a different place when it comes to election

security. That being said, I do believe that funds should be tied to a particular goal. An example of this is the requirement in the proposed Secure Elections Act that states use post-election audits. Because each state has unique considerations in its election laws and systems, each state may need to incorporate those considerations in any post-election audit procedure. Tying funds to a goal of each state conducting a statistically sound post-election audit can be achieved without specifying the exact audit procedures.

A balance needs to be struck between an encroachment on state authority over elections, and leaving states to fend for themselves in the face of another attempted intrusion by foreign actors. I believe the Secure Elections Act strikes the right balance. The Secure Elections Act provides floors, not ceilings, for state action to secure elections. It provides guidelines and best practices, while ensuring state control of elections.

What resources do state election officials currently have to evaluate cybersecurity products and service vendors?

Minnesota has a robust certification process for election equipment. First and foremost, Minnesota statutes require that a voting system must be certified by an independent testing authority accredited by the U.S. Election Assistance Commission (EAC) or appropriate federal agency. After the voting system is certified by the EAC, my office conducts its own certification and testing process before the continued use of the equipment.

For other election cybersecurity products, Minnesota does not have the same process. However, unlike many other states, Minnesota does not use vendors to support some of the main components of the state's election systems. For example, the second largest component of our election system, behind the actual equipment, is the Statewide Voter Registration System (SVRS). SVRS was built in-house using federal resources, and continues to be maintained in-house.

However, outside of the equipment certified by the EAC or the systems designed and maintained by my office, there are other systems and vendors for which we do not have the same transparency and evaluation resources.

Should the Department of Homeland Security or the Election Assistance Commission provide a clearinghouse of information, which includes vetting of vendors? Are the 'cyber navigators' and cyber liaisons appropriately serving a similar function?

The resources my office has received from both the U.S. Election Assistance Commission and the Department of Homeland Security have been incredibly helpful, but more information is always valuable, especially in light of the ongoing threats our elections face. While the cyber navigator can provide some additional information, I believe it would be helpful to have a central agency vetting vendors for minimum standards, much like the EAC does with voting equipment.

3) **In May 2018, the Senate Intelligence Committee released its first Unclassified Russia Report, which included recommendations on election security. In the report, it was found that DHS was not well-positioned to provide effective support to states confronting a hostile nation-state cyber actor. While early interactions between state election officials and DHS were strained, DHS has proven to have made progress in recent months. For one, DHS is now engaging more with state election officials, including providing necessary security clearances for these officials to ensure effective information sharing.**

How would you characterize states' engagement with DHS since 2016 – has it improved? Can you describe improvements in information sharing and the sharing of threat information?

Communication with the Department of Homeland Security, federal law enforcement, and other intelligence officials has improved dramatically since 2016. They have helped us, both in person and remotely, to identify potential vulnerabilities and best practices. Two high-level staff members and I have security clearances which allow us to receive regular briefings. With these security clearances, we are able to discuss potential threats and solutions collaboratively.

In addition to security clearances, in October 2017 the Elections Government Sector Coordinating Council (GCC) was established to ensure federal information and resources reached state and local election officials. The council, of which I am a member, allows for more collaboration between federal, state, and local officials to secure elections and share information in a timely manner.

Do your states' key election officials have security clearances so that you may discuss potential threats in a classified setting?

Yes, two high-level staff members and I have security clearances that allow us to receive regular briefings. With these security clearances, we are able to discuss potential threats and solutions collaboratively.

Do you believe that states should abide by any minimum standards when it comes to election security?

I believe that a balance needs to be struck between an encroachment on state authority over elections, and leaving states to fend for themselves in the face of another attempted intrusion by foreign actors. I believe any federal standards should provide floors, not ceilings, for state action to secure elections.

Senate Committee on Rules and Administration
Election Security Preparations: A State and Local Perspective
June 20, 2018
Questions for the record
Honorable Connie Lawson

Senator Wicker (R-MS)

1) As secretaries of state, you know more about the challenges facing your state than anyone else. We in Congress want to make sure your Federal partners are providing you with every possible resource to help you maintain the integrity of your data and election infrastructure. What areas do you feel Federal assistance is most needed and how would you like to see those resources distributed?

   To fully and completely fund:
   - The purchase of new election equipment;
   - The Election Assistance Commission for the purpose of administering distribution of funds and further support;
   - Staffing for the Department of Homeland Security for risk and vulnerability assessments, cyber hygiene support, etc.; and
   - Albert sensor purchases and ongoing monitoring and maintenance for county governments.

2) FOLLOW-UP: Some of my colleagues have introduced a bill that addresses some of the problems we are facing in protecting our election. Do you feel legislative action is necessary to address this issue, and do you think the Secure Elections Act is an adequate measure to help you face the coming elections?

   The Secure Elections Act is adequate, but measures should not encroach upon state responsibilities. We do not want the Secure Elections Act to duplicate efforts already underway in states and through the Government Coordinating Council, as this would be a waste of funding and time.

   It cannot be understated that we do not support the 'Hack the Election' or Defcon programs, as we wish to protect the clear responsibilities and security measures of individual states. These type of programs undermine confidence in election systems and disrupt the work of states, contractors, vendors, and partners. These programs have been overstated in value and lack real-world scenarios, presenting unrealistic electoral vulnerabilities.

Senator Warner (D-VA)

1) Provisions that address information sharing such as the Secure Elections Act would improve sharing of threat information from federal intelligence agencies with

appropriately cleared state and local election officials. However, information sharing is no cure-all, as there have been instances when state officials have misinterpreted relevant Indicators of Compromise in shared threat Intel reports, leading to confusion and potential misattribution. In addition, state officials have described the difficulty of prioritizing threats and keeping up with the vast amounts of information that is shared with them.

Could you describe how states and local officials are building the needed capabilities to intake, analyze, and operationalize threat information?

This question disregards the amount of time and effort – not to mention collaboration between the states and the Department of Homeland Security – invested in standing up election infrastructure, part of which was to establish communication protocols on what and how intelligence could be shared with Secretaries of State and state IT officials in an efficient manner. The question is inconsistent with efforts of the Government Coordinating Council and is ill-informed. We believe current communication protocols have the clarity we have sought since the threat arose in 2016.

Indiana passed a law during the 2018 legislative session that required local governments to report any security issues to the state. In addition, as we receive information from EI-ISAC, we share this information with state and county partners.

2) In the FY 2018 omnibus bill that passed this spring, $380 million in grant money was made available for states to help improve their election infrastructure.

Do you believe that election assistance funds should be tied to any particular actions on the part of states, or should they be spent as states see fit?

In most cases, $380 million, as distributed this spring, was not enough to purchase equipment. For Indiana, this represents 10% of what was initially disbursed in the original HAVA Act. We appreciate the need to attach reasonable conditions to federal funds, and could accept funds appropriated specifically for voter-verifiable paper trails, with a path for taking current DREs to a hybrid model allowing this. Any future funding should take the form of the HAVA funds, with oversight and support provided by the EAC.

However, it is difficult – even for large enterprises – to choose products and services that best meet their needs.

What resources do state election officials currently have to evaluate cybersecurity products and service vendors?

In addition to the Secretary's IT staff, the State utilizes resources from state agencies such as the Indiana Office of Technology, Indiana National Guard and IN-ISAC, as well as academia (Indiana and Purdue Universities). Additionally, the state utilizes its Voting System Technical Oversight Program, a program unique in the nation, and technical and program management organizations for research and tool comparison. Indiana regularly communicates with colleagues in other states.

Should the Department of Homeland Security or the Election Assistance Commission provide a clearinghouse of information, which includes vetting of vendors? Are the 'cyber navigators' and cyber liaisons appropriately serving a similar function?

I support an amendment that would require compliance with industry-standard security best practices. [NIST/VVSG?]

3) In May 2018, the Senate Intelligence Committee released its first Unclassified Russia Report, which included recommendations on election security. In the report, it was found that DHS was not well-positioned to provide effective support to states confronting a hostile nation-state cyber actor. While early interactions between state election officials and DHS were strained, DHS has proven to have made progress in recent months. For one, DHS is now engaging more with state election officials, including providing necessary security clearances for these officials to ensure effective information sharing.

   How would you characterize states' engagement with DHS since 2016 – has it improved? Can you describe improvements in information sharing and the sharing of threat information?

   It is problematic that the first congressional report was released in May 2018, almost two years after the 2016 elections. The expectation from Congress is that states will protect elections, yet Congress does not provide actionable intelligence to states. Congress must communicate in a timely manner with states in the same manner as DHS is expected to do. Resources states have received from DHS include improved communication, intelligence sharing, security clearances, and Election Day resources.

   Do your states' key election officials have security clearances so that you may discuss potential threats in a classified setting?

   Secretary Lawson has received a security clearance, and Chief of Staff and Director of IT are in the application process.

   Do you believe that states should abide by any minimum standards when it comes to election security?

Certainly, but what is the definition of 'election security'? Network security? Equipment security? We are far from a consensus on these and other definitions, which prohibits a constructive conversation on what any minimum standards might be. NASS, NASED, state and locals should be responsible for setting the standard.

Question#:	1
Topic:	Communication with State Officials
Hearing:	Election Security Preparations: A State and Local Perspective
Primary:	The Honorable Roger F. Wicker
Committee:	RULES (SENATE)

Senate Committee on Rules and Administration
Election Security Preparations: A State and Local Perspective
Post-election Audits
July 11, 2018
Questions for the record
Mr. Matthew Masterson

Question: We know that confidential voter information was accessed in at least two states leading up to the 2016 elections. Local and state officials have often expressed frustration at how little information they are given on cybersecurity threats known to the intelligence community in Washington. In fact, many secretaries of state have obtained "top secret" security levels to help curb these hacking attempts. However, it's our understanding that there is still little-to-none communication with DHS and state officials.

Can you comment as to why there has been little communication between local officials and Washington DC?

In your opinion, what can Congress do to ensure states are able to access the information they need to protect their elections?

Response: The Department of Homeland Security (DHS) has taken a number of steps to improve communication with state and local election officials over the past two years. DHS has moved quickly to establish and support the Election Infrastructure Subsector (EIS) which facilitates prioritizing existing resources, increasing our engagements with election stakeholders, and deploying a range of cybersecurity services to state and local partners

The National Protection and Programs Directorate (NPPD) engages directly with election officials to share information coordinate incident response, and provide other resources and services. In order to ensure a coordinated approach from the Federal Government, DHS established an Election Task Force (ETF) encompassing stakeholders from across the interagency. The ETF serves to provide election officials with actionable information and offer assistance to help local election officials strengthen their election infrastructure by reducing and mitigating cyber risk, and increasing resilience of their processes.

Question#:	1
Topic:	Communication with State Officials
Hearing:	Election Security Preparations: A State and Local Perspective
Primary:	The Honorable Roger F. Wicker
Committee:	RULES (SENATE)

In 2017, DHS created an ETF to improve coordination with and support to election stakeholders. The Task Force is focused on enhancing coordination between election officials, the intelligence community, and law enforcement partners to secure their systems. The Department has worked with federal, state, and local partners to establish the EIS Government Coordinating Council (GCC), which focuses on issues such as developing information sharing protocols and key working groups. Additionally, DHS has worked with a range of relevant private sector companies to establish a Sector Coordinating Council (SCC), which is focused on security issues relevant to private sector companies that support the operations of our election process. The EIS GCC and SCC work together to address the needs of the EIS.

In 2018, the Department also provided funding for the creation of the Election Information Sharing and Analysis Center and actively participates in sharing tailored election infrastructure cybersecurity information with state and local election officials on an ongoing and persistent basis. All 50 states and over 1,000 local jurisdictions have signed up to receive this information.

DHS has authority to make available the process and application for security clearance to state, local, tribal, and territorial government officials, and the private sector. As such, the Department has been working with state chief election officials to help them obtain security clearances in an expedited manner and has expanded the offer of security clearances to two additional officials in each state. Furthermore, DHS is assisting members of the more recently established SCC with obtaining security clearances. In partnership with the Office of the Director of National Intelligence and the Federal Bureau of Investigation, in February we gathered all state chief election officials at an intelligence community facility and provided one-time read-ins to a classified threat briefing. This was the first such gathering in our history.

Secretary Nielsen and other DHS senior officials have met with election stakeholders, including state election officials on multiple occasions to provide them with classified updates on the election threat. More recently – in August of 2018 - DHS undertook an unprecedented, first-ever national level table top exercise to address potential cyber threats facing election infrastructure on Election Day. Forty-four states and the District of Columbia took part in this exercise in addition to Federal government partners.

While there is more that could be done, it is critical that Congress pass the Cybersecurity and Infrastructure Security Agency Act. This law will establish a cybersecurity agency at the Department of Homeland Security to further the national effort to enhance the security and resilience of U.S. cyber and physical critical infrastructure

Question#:	2
Topic:	Information Flow
Hearing:	Election Security Preparations: A State and Local Perspective
Primary:	The Honorable Dianne Feinstein
Committee:	RULES (SENATE)

Question: What steps have you taken to increase the flow of information between the Department of Homeland Security (DHS) and state and local election agencies? Please detail all steps that DHS has taken in this regard.

Response: The Department of Homeland Security (DHS) has taken a number of steps to improve communication with state and local election officials over the past two years. DHS has moved quickly to establish and support the Election Infrastructure Subsector (EIS) which facilitates prioritizing existing resources, increasing our engagements with election stakeholders, and deploying a range of cybersecurity services to state and local partners

The National Protection and Programs Directorate (NPPD) engages directly with election officials to share information coordinate incident response, and provide other resources and services. In order to ensure a coordinated approach from the Federal Government, DHS established an Election Task Force (ETF) encompassing stakeholders from across the interagency. The ETF serves to provide election officials with actionable information and offer assistance to help local election officials strengthen their election infrastructure by reducing and mitigating cyber risk, and increasing resilience of their processes.

In 2017, DHS created an ETF to improve coordination with and support to election stakeholders. The Task Force is focused on enhancing coordination between election officials, the intelligence community, and law enforcement partners to secure their systems. The Department has worked with federal, state, and local partners to establish the EIS Government Coordinating Council (GCC), which focuses on issues such as developing information sharing protocols and key working groups. Additionally, DHS has worked with a range of relevant private sector companies to establish a Sector Coordinating Council (SCC), which is focused on security issues relevant to private sector companies that support the operations of our election process. The EIS GCC and SCC work together to address the needs of the EIS.

In 2018, the Department also provided funding for the creation of the Election Information Sharing and Analysis Center and actively participates in sharing tailored election infrastructure cybersecurity information with state and local election officials on an ongoing and persistent basis. All 50 states and over 1,000 local jurisdictions have signed up to receive this information.

DHS has authority to make available the process and application for security clearance to state, local, tribal, and territorial government officials, and the private sector. As such,

Question#:	2
Topic:	Information Flow
Hearing:	Election Security Preparations: A State and Local Perspective
Primary:	The Honorable Dianne Feinstein
Committee:	RULES (SENATE)

the Department has been working with state chief election officials to help them obtain security clearances in an expedited manner and has expanded the offer of security clearances to two additional officials in each state. Furthermore, DHS is assisting members of the more recently established SCC with obtaining security clearances. In partnership with the Office of the Director of National Intelligence and the Federal Bureau of Investigation, in February we gathered all state chief election officials at an intelligence community facility and provided one-time read-ins to a classified threat briefing. This was the first such gathering in our history.

Secretary Nielsen and other DHS senior officials have met with election stakeholders, including state election officials on multiple occasions to provide them with classified updates on the election threat. More recently – in August of 2018 - DHS undertook an unprecedented, first-ever national level table top exercise to address potential cyber threats facing election infrastructure on Election Day. Forty-four states and the District of Columbia took part in this exercise in addition to Federal government partners.

Question#:	3
Topic:	Voter Fraud
Hearing:	Election Security Preparations: A State and Local Perspective
Primary:	The Honorable Dianne Feinstein
Committee:	RULES (SENATE)

Question: At the June 20 hearing before the Committee on Rules and Administration, Missouri Secretary of State Jay Ashcroft stated that "the evidence indicates that voter fraud is an exponentially greater threat than the hacking of our elections."

Do you agree with Secretary Ashcroft's claim that "the evidence indicates that voter fraud is an exponentially greater threat than the hacking of our elections"?

If so, on what basis have you reached that conclusion?

Response: The Department of Homeland Security (DHS) does not investigate cases of voter fraud. Instead, the Department of Justice (DOJ) investigates and prosecutes such violations of federal law. As such, DHS defers to DOJ.

Question#:	4
Topic:	Election Security and Integrity
Hearing:	Election Security Preparations: A State and Local Perspective
Primary:	The Honorable Dianne Feinstein
Committee:	RULES (SENATE)

Question: Please explain the importance in terms of selection security and integrity of using two-factor authentication for state voter registration databases.

Please explain the importance in terms of election security and integrity of using voter-verified paper ballots.

Please explain the importance in terms of election security and integrity of conducting post-election audits.

Response: Post-election audits are one of the multiple checks and redundancies in U.S. election infrastructure that make it likely that a cyber manipulation of U.S. election systems intended to change the outcome of a national election would be detected. Checks and redundancies also include diversity of systems, non-Internet connected voting machines, pre-election testing, and processes for media, campaign, and election officials to check, audit, and validate results.

Additionally, the Department of Homeland Security supports the work of election officials on the Election Infrastructure Government Coordinating Council, who worked to develop voluntary guidance for use of the funds provided to election officials by the Elections Assistance Commission (EAC) through the Fiscal Year 2018 Consolidated Appropriations Acts. Auditability is a core part of this guidance document.

EAC, as the independent federal agency charged with assisting state and local governments with election administration is well-suited to provide additional, authoritative information in this space.

Question#:	5
Topic:	Analyzing Threat Information
Hearing:	Election Security Preparations: A State and Local Perspective
Primary:	The Honorable Mark R. Warner
Committee:	RULES (SENATE)

Question: Provisions that address information sharing such as the Secure Elections Act would improve sharing of threat information from federal intelligence agencies with appropriately cleared state and local election officials. However, information sharing is no cure-all, as there have been instances when state officials have misinterpreted relevant Indicators of Compromise in shared threat Intel reports, leading to confusion and potential misattribution. In addition, state officials have described the difficulty of prioritizing threats and keeping up with the vast amounts of information that is shared with them.

Could you describe how states and local officials are building the needed capabilities to intake, analyze, and operationalize threat information?

Response: The Department of Homeland Security facilitates cybersecurity information sharing with and among state and local election officials through a various methods, including through the Election Infrastructure Subsector Government Coordinating Council and the Election Information Sharing and Analysis Center. We work closely with state and local officials to ensure that this information is both actionable and relevant.

Question#:	6
Topic:	Election Assistance Funds
Hearing:	Election Security Preparations: A State and Local Perspective
Primary:	The Honorable Mark R. Warner
Committee:	RULES (SENATE)

Question: In the FY 2018 omnibus bill that passed this spring, $380 million in grant money was made available for states to help improve their election infrastructure.

Do you believe that election assistance funds should be tied to any particular actions on the part of states, or should they be spent as states see fit?

However, it is difficult - even for large enterprises - to choose products and services that best meet their needs.

What resources do state election officials currently have to evaluate cybersecurity products and service vendors?

Response: The $380 million was appropriated to the Election Assistance Commission (EAC). As such, the Department of Homeland Security defers to the EAC on the purposes for which the states used the funding.

Regarding existing resources available to states for vetting of cybersecurity products, states can use the General Services Administration Schedule and state-level procurement vehicles as one tool to evaluate such products.

Question#:	7
Topic:	Information Clearinghouse
Hearing:	Election Security Preparations: A State and Local Perspective
Primary:	The Honorable Mark R. Warner
Committee:	RULES (SENATE)

Question: Should the Department of Homeland Security or the Election Assistance Commission provide a clearinghouse of information, which includes vetting of vendors? Are the 'cyber navigators' and cyber liaisons appropriately serving a similar function?

Response: The Department of Homeland Security (DHS) does not provide a clearinghouse of information regarding vendors. However, DHS provides state and local election officials with threat information, advances risk management efforts, and prioritizes making available cybersecurity services.

In addition, there are existing resources available to states, such as the General Services Administration Schedule or state-level procurement vehicles that assist in vetting the technical competencies of some vendors.

The Department defers to EAC, as the independent federal agency charged with assisting state and local governments with election administration, to respond on their behalf.

Question#:	8
Topic:	Engagement with DHS
Hearing:	Election Security Preparations: A State and Local Perspective
Primary:	The Honorable Mark R. Warner
Committee:	RULES (SENATE)

Question: In May 2018, the Senate Intelligence Committee released its first Unclassified Russia Report, which included recommendations on election security. In the report, it was found that DHS was not well-positioned to provide effective support to states confronting a hostile nation-state cyber actor. While early interactions between state election officials and DHS were strained, DHS has proven to have made progress in recent months. For one, DHS is now engaging more with state election officials, including providing necessary security clearances for these officials to ensure effective information sharing.

How would you characterize states' engagement with DHS since 2016 - has it improved? Can you describe improvements in information sharing and the sharing of threat information?

Do your states' key election officials have security clearances so that you may discuss potential threats in a classified setting?

Response: The Department of Homeland Security (DHS) has taken a number of steps to improve communication with state and local election officials over the past two years. DHS has moved quickly to establish and support the Election Infrastructure Subsector (EIS) which facilitates prioritizing existing resources, increasing our engagements with election stakeholders, and deploying a range of cybersecurity services to state and local partners

The National Protection and Programs Directorate (NPPD) engages directly with election officials to share information coordinate incident response, and provide other resources and services. In order to ensure a coordinated approach from the Federal Government, DHS established an Election Task Force (ETF) encompassing stakeholders from across the interagency. The ETF serves to provide election officials with actionable information and offer assistance to help local election officials strengthen their election infrastructure by reducing and mitigating cyber risk, and increasing resilience of their processes.

In 2017, DHS created an ETF to improve coordination with and support to election stakeholders. The Task Force is focused on enhancing coordination between election officials, the intelligence community, and law enforcement partners to secure their systems. The Department has worked with federal, state, and local partners to establish the EIS Government Coordinating Council (GCC), which focuses on issues such as developing information sharing protocols and key working groups. Additionally, DHS has worked with a range of relevant private sector companies to establish a Sector

Question#:	8
Topic:	Engagement with DHS
Hearing:	Election Security Preparations: A State and Local Perspective
Primary:	The Honorable Mark R. Warner
Committee:	RULES (SENATE)

Coordinating Council (SCC), which is focused on security issues relevant to private sector companies that support the operations of our election process. The EIS GCC and SCC work together to address the needs of the EIS.

In 2018, the Department also provided funding for the creation of the Election Information Sharing and Analysis Center and actively participates in sharing tailored election infrastructure cybersecurity information with state and local election officials on an ongoing and persistent basis. All 50 states and over 1,000 local jurisdictions have signed up to receive this information.

DHS has authority to make available the process and application for security clearance to state, local, tribal, and territorial government officials, and the private sector. As such, the Department has been working with state chief election officials to help them obtain security clearances in an expedited manner and has expanded the offer of security clearances to two additional officials in each state. Furthermore, DHS is assisting members of the more recently established SCC with obtaining security clearances. In partnership with the Office of the Director of National Intelligence and the Federal Bureau of Investigation, in February we gathered all state chief election officials at an intelligence community facility and provided one-time read-ins to a classified threat briefing. This was the first such gathering in our history.

Secretary Nielsen and other DHS senior officials have met with election stakeholders, including state election officials on multiple occasions to provide them with classified updates on the election threat. More recently – in August of 2018 - DHS undertook an unprecedented, first-ever national level table top exercise to address potential cyber threats facing election infrastructure on Election Day. Forty-four states and the District of Columbia took part in this exercise in addition to Federal government partners.

Question#:	9
Topic:	Minimum Standards
Hearing:	Election Security Preparations: A State and Local Perspective
Primary:	The Honorable Mark R. Warner
Committee:	RULES (SENATE)

Question: Do you believe that states should abide by any minimum standards when it comes to election security?

Response: The Department of Homeland Security (DHS) does not set minimum security standards for state and local elections. DHS provides election officials and other stakeholders with recommended mitigation actions and best practices. Election officials are encouraged to implement this guidance consistent with their risk-based approach.

EAC, as the independent federal agency charged with assisting state and local governments with election administration is well-suited to provide additional, authoritative information in this space.

Senate Committee on Rules and Administration
Election Security Preparations: A State and Local Perspective
June 20, 2018
Questions for the record
Noah Praetz

Senator Feinstein

1) What steps have you taken to increase the flow of information between your agency and the Department of Homeland Security (DHS)?
ANSWER: I serve as co-chair of the Government Coordinating Council charged with helping DHS prioritize its actions and efforts with respect to election infrastructure. Our primary concern has been formalizing norms for information exchange. The GCC released a set of protocols and we were heavily involved in the effort to craft those. We are members of the ISAC and an Illinois based information sharing group that get us the information. But not all counties in Illinois get the data yet.

   Specifically, please provide the following information:

   a. Have you requested information from DHS about specific election vulnerabilities in your jurisdiction, including vulnerabilities in election infrastructure?
      i. Answer: Not outside of the Risk and Vulnerability Assessment of the Cook County infrastructure conducted by DHS.

   b. Have you shared information with DHS about specific election vulnerabilities that you have identified in your jurisdiction?
      i. Answer: No.

   c. Has DHS conducted a risk-and-vulnerability assessment of your voting jurisdiction? If not, have you requested DHS to conduct such an assessment?
      i. Answer: Yes they have conducted one already

2) The Consolidated Appropriations Act of 2018 included $380 million in funding available to be distributed to the states as HAVA Election Security Fund grants. Recognizing that you are county, rather than state, officials, please answer the following questions:

   a. To date, has your state requested any funding under the HAVA Election Security Fund grant program? If not, have you, as a county election official, pushed your state to request the HAVA funding to which it is entitled?
      i. Answer: Yes, our state has requested it. We did push hard. And we continue to push them very hard to spend it wisely.

b. If your state has requested funding, what improvements to election infrastructure and security have you undertaken with that funding? What improvements have other counties or voting jurisdictions undertaken?
   i. Answer: Illinois law requires that half of the HAVA funds be spent on procuring security expertise for the offices of local election officials through a "cyber navigator" Program that supports locals with experts. Those efforts will begin soon. Much of the remaining half of the funds will be distributed directly to the counties on a VAP basis – if they participate in the navigator program. We in suburban Cook County will use our portion to offset some of the costs of our ongoing acquisition of new voting equipment. We will also offset costs of acquiring and retaining cyber expertise. Finally, we will spend some of it on defense software tools and recoding.

c. If your state has not yet requested funding, do you know why? Do you know when your state plans to make formal request of the Election Assistance Commission (EAC) for such funding?
   i. Answer: NA

d. If you have not yet undertaken any improvements, how do you intend to use the funds allocated pursuant to the Consolidated Appropriations Act of 2018?
   i. Answer: NA

e. How much additional funding does your jurisdiction need to upgrade its election infrastructure?
   i. Answer: We need approximately $32 million to refresh our voting equipment over 10 years. We need approximately $2.5 million to employ appropriate security staff over 10 years. We need approximately $4 million to employ a variety of known mitigations and defensive tools and strategies.

3) At the June 20 hearing before the Committee on Rules and Administration, Secretary of State Ashcroft stated that "the evidence indicates that voter fraud is an exponentially greater threat than the hacking of our elections."

   a. Do you agree with Secretary Ashcroft's claim that "the evidence indicates that voter fraud is an exponentially greater threat than the hacking of our elections"?
      i. Answer: He used a calculation of 2 fraudulent votes versus 0 changed votes – and *technically* that's infinitely greater – but in either case I do not agree with him at all. While fraud is real, it is rare and focused on local elections from our experience. Further, measuring the effect of the hacking of our elections must be done on both fronts, the election infrastructure on one hand and the more successful influence campaign on the other. The influence campaign was clearly effective.

   b. If so, on what basis have you reached that conclusion?
      i. NA

4) Please explain the importance in terms of selection security and integrity of using two-factor authentication for state voter registration databases.
    a. Answer: We use two-factor authentication to interface with our state voter registration database and it has been effective in helping secure the system by adding some authentication credibility to users. However, in Illinois, our statewide system is primarily a copy of local systems' registration data and therefore the database of record is kept locally. This mitigates the effects of a successful breach of the statewide system.

5) Please explain the importance in terms of election security and integrity of using voter-verified paper ballots.
    a. Answer: Unlike nearly every other transaction in modern life, the security issues posed by the secret ballot requirement make voting uniquely reliant on a paper artifact for a trustworthy and transparent business process. There simply is no more satisfying way to assure the public that the software we use to count votes accurately identifies the winner of an election, than to conduct an audit by hand, comparing the actual paper artifact with the findings of the software, in respect to that same artifact. Nothing short of hand-counted audits will do. Every other type of audit is valuable and can add levels of confidence. And that may be enough for some folks. But to prove that the software identified the winner correctly, there is only one way – hand-counted audits of paper artifacts that were verified by the voters when they were cast.

6) Please explain the importance in terms of election security and integrity of conducting post-election audits.
    a. Answer: See answer to question 5 above.

<u>Senator Warner</u>

1) Provisions that address information sharing such as the Secure Elections Act would improve sharing of threat information from federal intelligence agencies with appropriately cleared state and local election officials. However, information sharing is no cure-all, as there have been instances when state officials have misinterpreted relevant Indicators of Compromise in shared threat Intel reports, leading to confusion and potential misattribution. In addition, state officials have described the difficulty of prioritizing threats and keeping up with the vast amounts of information that is shared with them.

Could you describe how states and local officials are building the needed capabilities to intake, analyze, and operationalize threat information?

A: Answer: The states approaching this problem correctly are building teams of security professionals who are partnering with local election officials. These partners, or "cyber navigators", are helping to improve defenses, including digesting information shared with election officials. They advance auditing and other verification techniques to ensure breaches are caught. And they are implementing plans to help with disaster recovery or business continuity when bad things happen.

2) In the FY 2018 omnibus bill that passed this spring, $380 million in grant money was made available for states to help improve their election infrastructure.

Do you believe that election assistance funds should be tied to any particular actions on the part of states, or should they be spent as states see fit?

A: Answer: That money was released without ties. It was leftover hanging chad and butterfly ballot money. However, there is no question in my mind that investors in election security, like taxpayers through federal spending, should see a return on that investment directly in the form of resilient practices. I believe that the federal government should require paper ballots and hand-counted audits in exchange for their investment – with some minor potential exceptions for military and overseas voters. So outfitted, our elections can be counted even in the event of a massively successful cyber attack against our vote counting software. No other solution offers the same guarantee.

However, it is difficult – even for large enterprises – to choose products and services that best meet their needs. What resources do state election officials currently have to evaluate cybersecurity products and service vendors?

A: Answer: It's true, this can be the wild west and is currently proving to be just that. DHS or EAC could play an important part in at minimum offering to vet companies hoping to serve in this capacity. And once the vet, or certify a company, they can post that preferred provider list. States and Locals should be allowed to contract with others, but a certification would go a long way towards ensuring best investments by states and locals. States and locals are looking for this service to be provided.

Should the Department of Homeland Security or the Election Assistance Commission provide a clearinghouse of information, which includes vetting of vendors? Are the 'cyber navigators' and cyber liaisons appropriately serving a similar function?

A: Answer. Yes; DHS and EAC should consider playing this role. I do not believe the "navigators" will be adequate in this regard. The "cyber navigators" are themselves vendors that need to be vetted. The EAC may have the capacity to do this. DHS seems to already work with many vendors who could provide these services across critical infrastructure sectors and so the more efficient certifying or vetting body would be the EAC.

3) In May 2018, the Senate Intelligence Committee released its first Unclassified Russia Report, which included recommendations on election security. In the report, it was found that DHS was not well-positioned to provide effective support to states confronting a hostile nation-state cyber actor. While early interactions between state election officials and DHS were strained, DHS has proven to have made progress in recent months. For one, DHS is now engaging more with state election officials, including providing necessary security clearances for these officials to ensure effective information sharing.

How would you characterize states' engagement with DHS since 2016 – has it improved? Can you describe improvements in information sharing and the sharing of threat information?

A: I believe that the real layer needing fortification is the local layer of government; not the states. And while the states can play a significant role, the success of such efforts is

really mixed. DHS is not built to support 8,800 local election officials directly. And therefore states, with the established relationships and controls are integral to getting this right. But only if they are doing the right things. Therefore, I do believe more could be invested in DHS so that it could play a bigger role in either helping states fortify their locals or, in lieu of strong state action, providing direct support. Progress has been made on the relationship between states and DHS. And the national tabletop exercise completed this week is a great example of smart investment. I'll note that relatively few locals were in the rooms with the state officials and there remains a significant gap between states and locals in awareness of the threat and of available resources. The states having guarded their territory so zealously in the past are the ones who now bear the brunt of explaining why they are not ensuring all of their locals are being pulled into all of the information sharing and planning exercises.

Do your states' key election officials have security clearances so that you may discuss potential threats in a classified setting?
Answer: I do not know whether our state's key election officials have clearances. I have received mine.

Do you believe that states should abide by any minimum standards when it comes to election security?
A: Standards are tricky. I think there certainly is a set of baselines and norms that all should follow. Negotiating those has proven difficult. Certainly, the iterations of the Secure Elections Act are a testament to that. In my mind, there are two bright lines. First, paper ballot artifacts with hand counted audits. Second, persistent access to a skilled Election Security Officer for every local election official. These two actions both cover the downside catastrophic risk of wholesale vote-counting software failure, and also decreases the likelihood of successful attack on any election-related digital infrastructure like websites and voter registration databases, not to mention voting equipment.

Senate Committee on Rules and Administration
Election Security Preparations: A State and Local Perspective
June 20, 2018
Questions for the record
Shane Schoeller

Senator Feinstein

1) What steps have you taken to increase the flow of information between your agency and the Department of Homeland Security (DHS)?

   Specifically, please provide the following information:

   a. Have you requested information from DHS about specific election vulnerabilities in your jurisdiction, including vulnerabilities in election infrastructure?

      We are currently working with them on vulnerabilities they identify that we need to be aware of and our Information Systems department uses that information to complete a thorough review.

   b. Have you shared information with DHS about specific election vulnerabilities that you have identified in your jurisdiction?

      We are in the process of completing our assessment and will share as we see the need to do so per the recommendation of our Information Systems department.

   c. Has DHS conducted a risk-and-vulnerability assessment of your voting jurisdiction? If not, have you requested DHS to conduct such an assessment?

      It has not occurred yet, but is planned for in the future upon the conclusion of our own assessment.

2) The Consolidated Appropriations Act of 2018 included $380 million in funding available to be distributed to the states as HAVA Election Security Fund grants. Recognizing that you are county, rather than state, officials, please answer the following questions:

   a. To date, has your state requested any funding under the HAVA Election Security Fund grant program? If not, have you, as a county election official, pushed your state to request the HAVA funding to which it is entitled?

      Yes

b. If your state has requested funding, what improvements to election infrastructure and security have you undertaken with that funding? What improvements have other counties or voting jurisdictions undertaken?

We have not received funding at this time.

c. If your state has not yet requested funding, do you know why? Do you know when your state plans to make formal request of the Election Assistance Commission (EAC) for such funding?

d. If you have not yet undertaken any improvements, how do you intend to use the funds allocated pursuant to the Consolidated Appropriations Act of 2018?

Without any specific dollar amount to be appropriated to our county, it is difficult to give too much specificity. It will be important to look at opportunities to upgrade our current cybersecurity protection efforts. If there are further funds available after that goal is met, then it would be important to improve voter accessibility at each of our polling locations as a county.

e. How much additional funding does your jurisdiction need to upgrade its election infrastructure?

That amount is yet to be determined.

3) At the June 20 hearing before the Committee on Rules and Administration, Secretary of State Ashcroft stated that "the evidence indicates that voter fraud is an exponentially greater threat than the hacking of our elections."

a. Do you agree with Secretary Ashcroft's claim that "the evidence indicates that voter fraud is an exponentially greater threat than the hacking of our elections"?

I am concerned about both as an election official who administers the election. Neither are acceptable and we must do all we can to prevent both from occurring. For example, we have more tools at our disposal to help prevent voter fraud when there is an attempt to cast fraudulent ballots. The same cannot be said if a cyberattack occurs as not all local election officials have access to the same resources to protect their voter data and voting equipment. Working together at the local, state and federal level to safeguard all voter data and voting equipment from cyberattacks, is in my opinion, essential to protecting the integrity of every election.

b. If so, on what basis have you reached that conclusion?

4) Please explain the importance in terms of selection security and integrity of using two-factor authentication for state voter registration databases.

Two-factor authentication is essential to protecting the database anytime a password is possibly stolen and helps guarantee the authenticity of the person using system has been given previous permission to access the database.

5) Please explain the importance in terms of election security and integrity of using voter-verified paper ballots.

The following remarks were part of my testimony submitted for the written record that answers the question.

"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."

6) Please explain the importance in terms of election security and integrity of conducting post-election audits.

The following remarks were part of my testimony submitted for the written record that answers the question.

"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."

Senator Warner

1) Provisions that address information sharing such as the Secure Elections Act would improve sharing of threat information from federal intelligence agencies with appropriately cleared state and local election officials. However, information sharing is no cure-all, as there have been instances when state officials have misinterpreted relevant Indicators of Compromise in shared threat Intel reports, leading to confusion and potential misattribution. In addition, state officials have described the difficulty of prioritizing threats and keeping up with the vast amounts of information that is shared with them.

   Could you describe how states and local officials are building the needed capabilities to intake, analyze, and operationalize threat information?

   We are in the very beginning stages of this with our Secretary of State and so it is too early to comment on this question.

2) In the FY 2018 omnibus bill that passed this spring, $380 million in grant money was made available for states to help improve their election infrastructure.

   Do you believe that election assistance funds should be tied to any particular actions on the part of states, or should they be spent as states see fit?

   There are three key priorities that I believe the election assistance funds should be prioritized for as a state:

   - **Assessing the vulnerabilities to cybersecurity threats and attacks for each election authority in each county where there are no dedicated resources available to help them do their own.**
   - **Updating the statewide voter registration system**
   - **Updating Election Equipment**

   However, it is difficult – even for large enterprises – to choose products and services that best meet their needs.

   What resources do state election officials currently have to evaluate cybersecurity products and service vendors?

   As a county election official, I am aware that our state works with federal agencies and third party vendors to ensure they are identifying potential vulnerabilities. They also work through a numerous vendor assistance opportunities to identity potential threats and vulnerabilities that need to be addressed.

Should the Department of Homeland Security or the Election Assistance Commission provide a clearinghouse of information, which includes vetting of vendors? Are the 'cyber navigators' and cyber liaisons appropriately serving a similar function?

Yes. A clearinghouse is essential to ensuring local election authorities do not invest in services or products that fail to protect and enhance their cybersecurity efforts.

3) In May 2018, the Senate Intelligence Committee released its first Unclassified Russia Report, which included recommendations on election security. In the report, it was found that DHS was not well-positioned to provide effective support to states confronting a hostile nation-state cyber actor. While early interactions between state election officials and DHS were strained, DHS has proven to have made progress in recent months. For one, DHS is now engaging more with state election officials, including providing necessary security clearances for these officials to ensure effective information sharing.

How would you characterize states' engagement with DHS since 2016 – has it improved? Can you describe improvements in information sharing and the sharing of threat information?

Based on recent conversations with Secretary Ashcroft and DHS Senior Cybersecurity Advisor, Matt Masterson, I have been pleased with the progress that has occurred in recent months.

Do your states' key election officials have security clearances so that you may discuss potential threats in a classified setting?

The Secretary of State has two individuals who I believe are dedicated to this issue as an office for our state.

Do you believe that states should abide by any minimum standards when it comes to election security?

Yes, so long as the standards are agreed upon first by state and federal officials.

ELECTION SECURITY PREPARATIONS: FEDERAL AND VENDOR PERSPECTIVES

WEDNESDAY, JULY 11, 2018

UNITED STATES SENATE,
COMMITTEE ON RULES AND ADMINISTRATION,
Washington, DC.

The committee met, pursuant to notice, at 10:31 a.m., in Room SR–301, Russell Senate Office Building, Hon. Roy Blunt, Chairman of the committee, presiding.

Present: Senators Blunt, Cruz, Capito, Wicker, Fischer, Klobuchar, Udall, Warner, King, and Cortez Masto.

Also Present: Senators Lankford and Wyden.

OPENING STATEMENT OF HONORABLE ROY BLUNT, CHAIRMAN, A U.S. SENATOR FROM THE STATE OF MISSOURI

Chairman BLUNT. Good morning. The committee will come to order.

It is great to welcome our witnesses today. I am particularly grateful that two of our colleagues from the Senate will start us off with some observations they have about this critically important issue.

Also, I am glad that my fellow Missourian, Scott Leiendecker, is here. I had a chance to learn more about his growing company in this area a few weeks ago, and look forward to his testimony, as I do the testimony of all the others.

This is the second in a series of hearings on election security. As we know, during the 2016 election cycle, state and local officials were tested like they had not been tested before. Even after the election, were more aware of the threats that were out there and their need to have better information about those threats, and more help as to how to deal with them.

At our last hearing, the local officials told us that they needed timely and actionable information. They needed cyber security resources as well as technical assistance.

Today, we turn to the Federal officials who are in charge of helping provide that kind of assistance and looking at how they can better provide those resources, as well as private sector election vendors.

Efforts to secure American elections are not new. Following the 2000 election, the 2002 Help America Vote Act established the United States Election Assistance Commission to assist states in replacing voting systems and improving election administration.

HAVA, as that bill was called, also created a partnership between the Election Assistance Commission and the National Institute of Standards and Technology to create guidance for voting systems and to certify those voting systems.

In January 2017, the Department of Homeland Security designated, after the election year had past, election infrastructure as critical infrastructure. We are now in the first election series since that designation was made.

At our last hearing, we heard how this designation would affect information sharing between state, local, and Federal Governments. Today, we look forward to hearing more about the other aspects of that designation, which is the formalization of information sharing and collaboration between private entities and the Federal Government through the Sector Coordinating Council.

More recently, in the Fiscal Year spending bill, Congress appropriated $380 million to the U.S. Election Assistance Commission to help states enhance their election infrastructure. About 49 states and territories have already requested approximately $350 million of that money. In many cases, they have already received the money they have asked for.

Some of our goals today are to:

- Find out more about the tools that are available that the Federal Government can provide state and local officials;
- Find out about information sharing that is occurring and should occur between state, Federal, and local election officials;
- To learn more about what we might do to encourage cyber security best practices.

We are also pleased to have, again, Senator Wyden and Senator Lankford here. But before I turn to them, I will turn to Senator Klobuchar for any opening remarks she wants to make.

OPENING STATEMENT OF HONORABLE AMY KLOBUCHAR, A UNITED STATES SENATOR FROM THE STATE OF MINNESOTA

Senator KLOBUCHAR. Thank you, Mr. Chairman, for holding this important hearing.

Thank you, to all of you.

I would like to also thank Senator Wyden for being here. I am glad this worked out, and Senator Lankford for your work. I know you are both on the Intelligence Committee.

I know how incredibly important this topic is, and how there is a lot of focus on what has happened and what did happen. There should be. But we also have to keep our eyes moving forward on how we protect ourselves from this not happening again.

I am particularly pleased with the work that Senator Lankford and I have done on the Secure Elections Act, as he will describe. This legislation would improve government sharing between election officials and the Federal Government, provide vital resources and expertise to states, and make it easier to confirm election outcomes should there be back-up paper ballots audits.

The legislation has significant bipartisan support. We have painstakingly spent the last 18 months working with state and Federal officials. I know we have made significant changes to the legislation in listening to people, especially to the secretaries of states, around the country to meet their concerns.

It is truly vital that we work together, and this is one effort, but there are so many others going on, especially with the way the Intelligence Committee has handled this investigation, the way Senator Blunt and I want to handle this going forward on the election side. It is truly important that this be bipartisan.

We had it in a hearing in front of Judiciary recently and it became very clear that while a lot of the focus on the interference has been about the general election in 2016, it was also going on in the

primary, specifically targeted at Senator Rubio's campaign and others.

I think it is very important for us to keep telling those stories and to remind ourselves that it was not just going on with one party versus another. They were doing things that affected the primary. They were doing things that were actually outside of the actual election involving causes, and groups, and people, and trying to turn people against each other basically; whether it was the pipeline in North Dakota or whether it was rallies in Florida.

The state and local election officials who are administering elections on the frontlines, they are working hard to ensure our election systems are secure. I know my Secretary of State, Steve Simon, who was here recently, would tell you that he and his colleagues across the country are all very focused on this.

During our hearing last month, we heard from some of those officials about the challenges they face and the need for additional resources in light of the continuing threat posed by Russia and other potential adversaries.

Today, we will hear from Federal officials and representatives from voting systems companies. Currently, over 90 percent of Americans vote on machines from three companies. I am pleased that one of these companies, Hart InterCivic, is here today, but I wish that the other two companies could have also joined us.

Given the threats we face, and the billions of Federal and state tax dollars that go to these companies, oversight is vital to ensure that they are providing secure and reliable voting machines and services to others.

Congress must do everything we can to defend our elections and bolster Americans' confidence in our democratic process.

I am glad we have a diffuse system with different systems in different states' jurisdictions because then one hack will not ruin everything. But we know that one hack in one county in one state will jar peoples' confidence. They came close last time trying to hack into 21 states, got as close as the voter list in Illinois, and we just do not want this to happen again.

Thank you very much, Mr. Chairman.

Chairman BLUNT. Well, thank you, Senator Klobuchar, and I look forward to working with you on this.

Certainly, we have both worked with Senator Lankford and Senator Wyden, who are on Intelligence with me, care deeply about these issues, have had lots of time to think about them. We are glad they are here to share some of those thoughts today.

Senator Wyden, if you would like to start, I would like for you to go first.

OPENING STATEMENT OF HONORABLE RON WYDEN, A UNITED STATES SENATOR FROM THE STATE OF OREGON

Senator WYDEN. Thank you very much, Mr. Chairman.

Mr. Chairman, first, let me thank you for your thoughtfulness in making it possible for me to come today, and I very much look forward to working with you.

Senator Klobuchar and I have discussed these issues as well over the years.

Mr. Chairman, you have a busy schedule, so I am just going to try and make a few key points.

According to the latest numbers, at least 44 million Americans, and perhaps millions more, have no choice but to use insecure voting machines that make hackers and hostile foreign governments salivate.

It is, in my view, inexcusable that our democracy depends on such hackable voting technology made by a handful of companies that have been able to evade oversight. In fact, have actually been stonewalling the Congress for years.

The efforts by Russia, obviously, during the 2016 election highlight the vulnerability of our election infrastructure and the serious threats that our people face.

As you and I talk, Mr. Chairman, I recently introduced a new cyber security bill to focus on the reliability and accuracy of Federal elections. It seems to me enormously important, given the prospect that these foreign hackers can get access and can hack the voting machines used by the states.

My legislation focuses on two common sense measures that are backed by the overwhelming number of cyber security experts in our country: Paper ballots and risk-limiting audits.

I wrote this bill in spite of this campaign of ducking, and bobbing, and weaving, really stonewalling from the major voting machine companies. Over the past year you and I have touched on this as a member of the Intelligence Committee—I reached out to cyber security experts, election officials, and others.

I wrote the big voting machine companies asking them basic questions about their cyber security. These were not complicated questions. They were, "Have you been hacked?" "Do you employ in-house cyber experts?" Really, the basic, sort of "cyber hygiene 101."

The companies refused to answer how or even if they are protecting their systems and the votes of the American people.

Earlier this year, "The New York Times" published a story revealing that ES&S, the largest voting machine manufacturer, was selling devices that came preinstalled with modems and remote monitoring software. The experts say remote access to election infrastructure is now a five-alarm crisis when it comes to security.

My view is you could only make it worse if you were to leave unguarded ballot boxes in Moscow and Beijing. I kept writing to the company, following up with the same common sense questions. They ignored those as well.

It is clear to me, Mr. Chairman, these companies want to be gatekeepers of our democracy, but they seem completely uninterested in safeguarding it.

Five states exclusively use voting machines that do not produce a paper trail. The only record of the votes cast is a digital record, which could be hacked and which is impossible to audit reliably. That strikes me as a prescription for disaster.

Americans need to have paper ballots marked by hand. Until that system is adopted, every election that goes by is yet another election that foreign governments, hostile foreign governments including Russia, can hack.

Earlier this year, the Congress appropriated $380 million to help states upgrade their election technology. The money is now in the

hands of the Election Assistance Commission and on the way to the states. It ought to be used to bolster security. Unfortunately, it is not clear at all how the Election Assistance Commission is actually using the money to do this.

My concern, as you and I have talked about, Mr. Chairman, is the states could go out and buy a whole lot more hackable technology from these stonewalling voting machine companies.

Let me just wrap up by saying before we conclude, the statements of the Commissioner who is number two at the commission, Commissioner McCormick, also concern me greatly. She stated publicly last year that she disagrees with the intelligence community that Russia sought to influence the 2016 election.

Mr. Chairman, you and I have heard again and again that it is the view, and Senator Lankford has heard this as well, it is the overwhelming view of the intelligence community that Russia sought to influence the 2016 election. I cannot for the life of me figure out why the number two official of the Election Assistance Commission is dismissing the analysis of the Government's and the Administration's intelligence experts.

You can set aside the outcome of the 2016 election. No matter who you pulled the lever for the last time around, all of us here in the Senate have to care about defending our elections from foreign hackers going forward.

Again, Mr. Chairman, I want to thank you for your courtesy and the time you and I have spent talking about this.

I look forward to working with you in the days ahead.

Chairman BLUNT. Well, I look forward to you and I continuing to work on this, Senator Wyden, as I do with Senator Lankford.

Senator Lankford, we are pleased you are here this morning as well.

Senator WYDEN. Mr. Chairman, I just want to apologize to my colleague for ducking out because I know he has something important to say. The Finance Committee is pending.

I thank my colleague, and the Chair, and the Ranking Member.

OPENING STATEMENT OF HONORABLE JAMES LANKFORD, A UNITED STATES SENATOR FOR THE STAKE OF OKLAHOMA

Senator LANKFORD. Mr. Chairman, thank you for inviting me back again to the Rules Committee. It is good to be back in this conversation again. There is a lot that still needs to be done.

Senator Klobuchar and I have worked very hard on the Secure Elections Act. This has been a work in progress that was written in pencil, so it could be used to be able to be erased, edited, rewritten, re-erased, reedited over and over again as we have gone through this multiple iterations of the Secure Elections Act.

We do need to deal with the obvious threats that are coming at our Nation dealing with elections. We should have learned the lesson from 2016. Though this will take a long time to be able to roll out real results and responses over the course of our Nation, we do need to deal with these threats.

The Secure Election Act tries to go focus on improving the ability of the states to be able to counter issues and threats that they face in the elections. Let me reiterate this.

I have absolutely zero doubt that the Russians tried to influence our elections; that they were trying to engage in any way that they could to bring instability to our democracy. But I also have no question that our states are not only qualified to be able to handle the elections, but they are constitutionally responsible to be able to handle our elections. The states need to be able to continue to control elections.

With Senator Klobuchar and others, what we have worked on together is to be able to form how do we head off this issue from coming at us again. It is not so much about the next election because, quite frankly, there is a lot of attention being paid to the next election.

It is what is the election structure 20 years from now? Will we let our guard down? Will the focus not be there? To be able to put some processes in place to say, "How do we make sure 20 years from now, we have not forgotten the lessons that we should have learned from 2016?"

Some basic things have come out of that conversation. One is increasing the communication between the Federal Government and states. There was not near enough communication between the Federal Government and the states leading up to the 2016 time period.

We also discovered there was not security clearance for individuals in the states, so when issues were discovered, there was no one to be able to communicate that with quickly that already had clearance.

Many elections across the Nation do not have auditable elections. They are done completely electronically and there was no way to be able to audit it at the end of the election and determine did everything go correctly? It was simply a best guess of, "Yes, everything looks like it went correctly," but there was no way to really know.

There are many states that do risk-limiting audits after the election is over, but some states do not. When it is a Federal election, it is difficult if there is a threat to any one entity in any one state. That affects every other state as well.

There are some basic things that can be done that we feel could be done and could be done still allowing states to be able to control their election structure, and to have flexibility on the type of election machines they want to have and the type of election systems that they want to have. It should be completely up to the states to be able to run that.

Senator Klobuchar and I have worked very hard and have refined the Secure Elections Act. We have had a tremendous amount of feedback, as Senator Klobuchar mentioned before, from secretaries of states and heads of elections officials from the EAC and the DHS.

We met with a bipartisan group of state secretaries in April, including the president of the National Association of Secretaries of State, Secretary Ashcroft from Missouri, Secretary Schedler from Louisiana, and Secretary Simon from Minnesota when we incorporated their advice.

We have exceptional feedback, quite frankly, from the Chief Election Official in my state, Paul Ziriax, as well as former Election Assistance Commissioner Matt Masterson.

We have also talked extensively to Secretary Nielsen from DHS and received a tremendous amount of feedback as well what DHS is doing.

We do want to be able to see improvements and we do believe the coordinating councils can share a lot of that information with other states and with the Federal Government. But there are some simple things that can be in place that we feel do not usurp the authority of the states to be able to run their own elections, but do give us a secure election system for the future.

Again, the issue is not so much 20/20. We are all paying attention and we are all watching. What would the elections be like 20 years from now? Will we still have a process in place that protects the elections when our guard is down?

We think it is a wise idea to be able to continue that ongoing cooperation and communication so when issues are discovered, it can be shared state to state quickly. It can be shared from the state to the Federal Government and the Federal Government to the states. To be able to make sure we continue to protect our elections and to make them as secure as possible.

Mr. Chairman, thank you, again for the invitation to be here and it is my honor to be able to join this conversation if only for a brief moment.

Thank you for holding this hearing because this will be exceptionally important that we actually get a bill across the floor, get it passed, and to be able to help secure our elections for the future.

Thank you.

Chairman BLUNT. Thank you, Senator Lankford.

We will call our first full panel up, we do have two panels this morning, and that will be Chairman Hicks and Commissioner McCormick, along with Dr. Romine from the National Institute of Standards and Technology, and Mr. Masterson from the Department of Homeland Security.

I would say, as you are coming up and we are getting nameplates up, that your full statement will be in the record. We do, as I mentioned before, have another panel after you and we certainly want to have a chance to ask questions.

You can deal with your time however you would like to, but if you want to summarize anything in your statement, we will have your statement in the record, and we are glad to have it, as we are glad to have you here today.

We will start, Chairman Hicks, the Chairman of the Election Advisory Commission with you and then go to Commissioner McCormick, and then Dr. Romine, and Mr. Masterson.

Chairman Hicks.

OPENING STATEMENT OF COMMISSIONER THOMAS HICKS, CHAIR, U.S. ELECTION ASSISTANCE COMMISSION, SILVER SPRING, MARYLAND

Mr. HICKS. Good morning, Chairman Blunt, Ranking Member Klobuchar, members of the committee.

I am pleased to testify before you today to discuss the U.S. Election Assistance Commission's work to support state and local election leaders in their efforts to conduct efficient, accessible, and secure elections.

The Commission takes great pride in the resources and assistance we provide to election officials and voters, as well as the vital role we play as a national clearinghouse of election administration information to our partners in Congress, other Federal agencies, state and local governments, private industry, advocacy organizations, academia, and others in the election industry.

As emphasized by witnesses at the last election related hearing, the EAC is focused solely on elections serving as an essential hub for other Federal agencies that spend only part of their time working on this important issue, including those who specialize in technology and cyber security.

Our partners, ranging from the Department of Homeland Security, the Federal Bureau of Investigation, the U.S. Postal Service, and the DOD, rely on the EAC to provide a deep knowledge of how elections work and a clear line of communications to those in the field who administer the vote.

Most recently, our partner agencies have counted on the EAC to fulfill this role with regard to election security. This topic is not new to the state and local election officials who run elections, the tens of thousands of election administrator staff, and election workers who support that work. It has long been a primary focus for the men and women on the frontlines of elections. Something they think about 365 days a year and during a Presidential year 366 days a year.

The job description of the election official is everything from ADA compliance and voter registration to mail management and human resources. This is why it is so vital that Congress and the Federal agencies, especially EAC, provide election administrators with the resources and tools they need to succeed.

The establishment of election systems is part of the Nation's critical infrastructure was one way the Federal Government sought to improve the mechanisms it uses to accomplish this goal. In many ways, the EAC's work during the 2016 Federal election set a fundamental effort for this.

At that time, prior to the critical infrastructure designation, we worked with DHS and the FBI to distribute security alerts and threat indicators to state and territories to help protect election systems from specific cyber security threats.

We also met this goal with our Federal partner agencies by meeting with the White House to discuss these threats to the election systems, the security protocols, and the dynamics of the election system in the 8,000-plus jurisdictions nationwide.

Following former Secretary Johnson's critical infrastructure announcement, the EAC actively worked to provide state and local election officials with a voice at the table during this discussion and how the sector would function.

DHS has often stated that the Sector's Government Coordinating Council, the GCC, was formed faster than any other similar critical infrastructure sector council to date. The EAC takes great pride in this role, one that we played to make that happen.

It is proof of how local, state, and Federal Governments can effectively work together towards a common goal of protecting our Nation's infrastructure. I serve on the GCC's executive committee, which has worked diligently to ensure the critical infrastructure designation has a tangible, meaningful impact across our Nation.

We all know that there are many solutions to the security challenges, but it takes resources. We were pleased that the members of this committee, and your congressional colleagues, recognized this reality when supporting the Congressional Appropriations Act of 2018.

That legislation contained $380 million for the states and territories to improve the administration of Federal elections. Just 3 months after that appropriation bill was signed into law, the EAC has received requests from more than 97 percent of those funds from 51 of the 55 states and territories designated to receive funds.

That is a remarkable percentage and demonstrates the EAC's responsiveness and the states' urgency in addressing methods to make election systems more resilient.

Less than 2 weeks after President Trump signed the appropriations bill into law, the EAC personally notified each eligible jurisdiction and issued grant award letters to every state and territory.

Just 1 week after that, your home state, Mr. Chairman, Missouri, received its funds. It was the first state to request its funds and receive its funds.

In the weeks that followed, the EAC conducted a Webcast public forum and explained the funds and worked directly with NAS, NAS head to share this information. The EAC also conducted webinars, published FAQ's, and other resources on our website, and educated nongovernmental groups including those focused on accessibility and security. Our expert grants administration team has also helped states navigate this hurdle.

On behalf of the states and territories, I want to thank you again for these vital resources, and I assure you that they are being put to good use. Our Vice Chair, Commissioner McCormick, will detail some of the efforts for you.

In the meantime, I want to thank you again for inviting the EAC to testify today, and I look forward to answering any, and all, of your questions.

[The prepared statement of Mr. Hicks was submitted for the record.]

Chairman BLUNT. Thank you.

Commissioner McCormick.

OPENING STATEMENT OF COMMISSIONER CHRISTY MCCORMICK, VICE CHAIR, U.S. ELECTION ASSISTANCE COMMISSION, SILVER SPRING, MARYLAND

Ms. MCCORMICK. Chairman Blunt, Ranking Member Klobuchar, and members of the committee.

Thank you for inviting the EAC to testify today about the vital issue of election security.

My name is Christy McCormick and I am a former Chair of the EAC, and currently serve as the Vice Chair, and I have been working in elections for three decades, starting out as a local voter registration assistant.

When Congress passed the Help America Vote Act of 2002, it established the EAC as an independent, bipartisan commission charged with developing guidance to meet HAVA requirements; adopting voluntary voting system guidelines, and certifying election systems; serving as the national clearinghouse of information on election administration; as well as dispensing and auditing HAVA funds.

I am pleased to report that our capable team continues to fulfill this mission and that election officials across the Nation consistently affirm that our work does indeed help America vote.

Today, I will focus my remarks on the impact of the newly appropriated HAVA funds and the EAC's efforts to supplement these resources.

As Chairman Hicks noted, states and territories are wasting no time in applying for their portion of the $380 million that was appropriated in March. This is no surprise.

The U.S. election officials are well known to be resourceful, dedicated, and innovative. Their work to serve American voters, and to protect the integrity of elections, is deserving of our praise and support. Thanks to them, election systems from coast to coast produced accurate results in 2016 and were resilient in the face of reported security threats.

I have every confidence that the newly appropriated HAVA funds are helping officials to continue this vital work to strengthen their systems ahead of this year's midterm election and the 2020 Presidential election.

While election officials are continuing to work with state legislators, local elected leaders, advocates, and other stakeholders to fine tune how they will spend these funds, today, I will provide a brief snapshot of some of the efforts we know are already underway to make the Nation's election systems more accessible, efficient, and secure.

South Dakota is using the $3 million it received to upgrade voting equipment including ballot marking devices and ballot tabulators. Their existing equipment was purchased in 2005. The state will make crucial cyber security upgrades to its statewide voter registration file and election night reporting page.

New York received over $19 million. The state plans to use this infusion of funds to implement a state and local cyber security risk assessment program, remediate identified vulnerabilities, monitor ongoing security operations, and respond to incidents, should they occur.

In West Virginia, the Secretary of State's office developed a plan after surveying local election officials for cyber and physical security assessments. The state will increase election system protections, bolster protection capabilities, and prepare for corrective action, if necessary.

The territories, many of which suffered catastrophic damage during last year's hurricane season, are especially grateful for their HAVA funds.

For example, ahead of this year's midterm election, American Samoa is using a portion of the $600,000 that they received to restore the territory's election office and to replace equipment damaged during Tropical Cyclone Gita.

They are upgrading their voter registration system, increasing accessibility at the polls, broadening voter education efforts, and improving election workstations and data bases.

As part of the EAC's clearinghouse function, we are highlighting each state's initiatives so other jurisdictions may refer to them as they might determine the best ways to utilize their appropriated funds.

Right now, the EAC's priority is to get these funds out the door as quickly and responsibly as possible. I am pleased to report that we are, indeed, meeting that challenge.

The EAC has a broad spectrum of ongoing work that complements our role as the administrator of HAVA funding. We kicked off 2018 with an election summit that convened election administrators, security experts, academics, Federal Government officials, and many others to discuss approaches to strengthen election systems and better serve American voters.

Building on the momentum coming out of that event, the EAC has continued to release new resources, conduct trainings, and participate in initiatives focused on election security.

For example, EAC staff has traveled to nearly a dozen states to present, "Election Officials as IT Manager," trainings for state and local election officials. These trainings are ongoing and we are working with DHS to put the training online through the FedVTE platform.

Chairman Hicks and I regularly travel to election jurisdictions throughout the Nation where we meet with state and local election officials and hear firsthand how our commission, and the Federal Government, may improve the assistance that we provide.

We also conduct public hearings and forums to gather feedback. For example, earlier this year, the EAC held a public forum to discuss the HAVA funding and to hear from election officials about ways they are working to secure their systems and improve their processes.

Most recently, we held a public forum in Baltimore where hundreds of Americans with disabilities were gathered for the National Disability Rights Network's annual conference. At that gathering, we addressed the need to secure election systems consistent with the legal requirements that ensure voters can cast their ballots privately and independently.

The EAC plays the unique role as the only Federal entity solely focused on the administration of elections. We appreciate Congress' support of our efforts in the states and territories we serve.

I look forward to providing additional details about the commission's work and answer any questions that you have.

[The prepared statement of Ms. McCormick was submitted for the record.]

Chairman BLUNT. Thank you, Commissioner.

Dr. Romine.

OPENING STATEMENT OF CHARLES H. ROMINE, PH.D., DIRECTOR, INFORMATION TECHNOLOGY LABORATORY, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, GAITHERSBURG, MARYLAND

Dr. ROMINE. Chairman Blunt, Ranking Member Klobuchar, and members of the committee.

I am Charles Romine, the Director of the Information Technology Laboratory at the National Institute of Standards and Technology, known as NIST.

Thank you for the opportunity to appear before you today to discuss NIST's role in election security.

NIST's role in helping secure our Nation's voting systems draws on our expertise in measurement science; in working with standards and development organizations, and stakeholder communities; and in the development of testing infrastructures necessary to support the implementation of standards.

Additionally, our experience working in multi-stakeholder processes is critical to the success of NIST's voting program.

For more than a decade, the NIST voting program has partnered with the Election Assistance Commission, or EAC, to develop the science, tools, and standards necessary to improve the accuracy, reliability, usability, accessibility, and security of voting equipment used in Federal elections for both domestic and overseas voters as outlined in the Help America Vote Act of 2002, or HAVA, and the Military and Overseas Voter Empowerment Act.

HAVA authorized NIST to provide technical support to the EAC's Federal Advisory Committee. The support includes intramural research and development to support the development of a set of voluntary voting system guidelines that are then considered for adoption by the EAC.

The first set of guidelines was adopted in 2005, and they significantly increased security requirements for voting systems. Version 1.1 of the guidelines was approved in 2015 and NIST immediately began work on the next iteration of the guidelines, Version 2.0.

The guidelines are used by accredited testing laboratories as part of both state and national certification processes by state and local election officials, who are evaluating voting systems for potential use in their jurisdictions, and by manufacturers, who need to ensure that their products fulfill the requirements to be certified.

The guidelines address many aspects of voting systems, including determining system readiness, ballot preparation, ballot counting, safeguards against system failure, and tampering and auditing.

NIST established a set of public working groups to gather input from a wide variety of stakeholders on the development of the next iteration of the guidelines 2.0. There are currently 963 members across seven working groups, three of which are in the election process; three groups focused on cyber security, usability and accessibility, and interoperability; and one that will address issues related to testing.

The Cyber Security Working Group has grown to 162 members and engages in discussions regarding the security of the U.S. elections.

As U.S. election infrastructure has evolved, so have its security concerns, which today range from unauthorized attempts to access

the voter registration systems of multiple states, to errors or malicious software attacks.

The guidelines address these evolving concerns, including support for advanced auditing methods and two-factor authentication that security protections developed by industry over the past decade are built-in to the voting system.

Other security issues to be resolved include the need for regular and timely software update and security patches. Networked communication is another important security issue currently under discussion. Many election jurisdictions rely on public telecommunications networks for certain election functions, such as reporting results to state agencies and media outlets the night of an election. These connections, however brief, are a significant expansion of threat surface and their security requires further study.

In January 2017, the Secretary of Homeland Security designated the Nation's election infrastructure as critical infrastructure. In support of this effort, NIST is providing technical leadership in the creation of an Election Profile of the NIST Cyber Security Framework. This profile is another tool NIST developed to help election officials identify and prioritize opportunities to improve their cyber security posture.

NIST also conducts evaluations of independent laboratories and provides the EAC a list of those laboratories proposed to be accredited. NIST developed uniform testing for critical security, usability, accessibility, and functionality requirements to achieve uniformity in testing among laboratories.

NIST is addressing election security by strengthening the Voluntary Voting System Guidelines for voting systems, and by working with our Government partners to provide guidance to state and local election officials on how to secure their election systems, including voter registration and election reporting systems.

Thank you for the opportunity to testify on NIST's work regarding election security.

I will be pleased to answer any questions that you may have.

[The prepared statement of Dr. Romine was submitted for the record.]

Chairman BLUNT. Thank you, Dr. Romine.

Mr. Masterson.

OPENING STATEMENT OF MATTHEW MASTERSON, SENIOR CYBER SECURITY ADVISOR, U.S. DEPARTMENT OF HOMELAND SECURITY, WASHINGTON, D.C.

Mr. MASTERSON. Thank you, Chairman Blunt, Ranking Member Klobuchar, and members of the committee.

Thank you for today's opportunity to testify regarding the Department of Homeland Security's ongoing efforts to assist state and local election officials, those who own and operate election systems, with improving the resilience of America's elections.

Today's hearing is timely. Later this week, DHS senior leadership will meet with election officials and their private sector partners as they gather in Philadelphia, the birthplace of our democracy, for their national summer conference and meetings of both our coordinating councils.

Throughout my career, I have worked with state and local election officials to advance the use of technology to better serve American voters. For the last three years, I served as a Commissioner at the Election Assistance Commission and now I serve as the Senior Advisor at DHS focused on the work the Department is doing to support the thousands of election officials across this country.

In this decade of work, I can tell you the best part is working with the dedicated professionals who administer elections. In the face of real and sophisticated threats, these officials have responded by working with us, state and local resources, the private sector, and academia to mitigate risks and improve resilience.

The risks to elections are real. The 2018 midterms remain a potential target for Russian actors. While we have yet to see any evidence of a robust campaign aimed at targeting our election infrastructure like in 2016, the intelligence community continues to see Russia using social media, false flag personas, sympathetic spokesmen, and other means to influence or inflame positions on opposite ends of controversial issues.

We remain vigilant and will continue to work with our election partners to strengthen the resilience of our election systems. As I travel the country working with state and local officials, it is clear that they are taking these risks seriously.

For example, Florida's election officials are engaged with DHS and the University of West Florida to conduct robust trainings across the state. In addition, the State of Florida and its supervisors became the first state to have every county join our elections information sharing center. We are currently working with Florida counties to employ network sensors across the entire state. There is remarkable progress in a short amount of time.

Our mission at DHS is to ensure that our stakeholders have the necessary information and support to assess and mitigate risks. We have made significant progress. State and local officials, as well as those private sector partners who support them, are at the table working with us.

We have created government and private sector councils who collaboratively work to share information and best practices. We have created the Election Infrastructure Information Sharing and Analysis Center, or EI-ISAC, growing to almost 1,000 members, including all 50 states, in just under 5 months. This is unprecedented growth compared with other sectors.

Since February 2018, working with EI-ISAC, we have quadrupled our awareness into election infrastructure through network monitors known as Albert sensors.

We are sponsoring security clearances for multiple election officials in each state, which allow officials to receive classified threat information.

We have increased the availability and deployment of free technical services to election officials. DHS offers a variety of services, such as cyber security assessments, intrusion detection capabilities, information sharing and awareness, incident response and training. Our suite of services will continue to mature as the requirements identified by our election stakeholders mature.

We understand the only way to deliver a resilient election system is to work collaboratively with those officials on the frontlines running the process.

DHS has been leading an interagency effort to support state and local officials through an elections taskforce. This taskforce brings together the Election Assistance Commission, NIST, the FBI, the intelligence community, and DOD. The purpose of the taskforce is to ensure that information is actual and timely shared broadly across the election sector.

The two partners sitting at the table with me now, EAC and NIST, have been invaluable resources for DHS as we have worked to develop and grow the maturity of this sector.

For example, as Dr. Romine referenced, we are working with NIST and the EAC, along with our Government Coordinating Council, to utilize the NIST framework to further empower election officials to better secure their systems.

The Department will continue to coordinate and support state and local officials to ensure the security of our election infrastructure. Malicious cyber actors can come from anywhere, within U.S. borders or from abroad. We are committed to ensuring a coordinated response from all levels of government. We understand the only way to do this is to work collaboratively with those officials that run the elections process.

Before I conclude, I want to take a moment to thank Congress for the legislative progress thus far in strengthening DHS' cyber security and critical infrastructure authorities. Specifically we strongly support passage of legislation to create the Cyber Security and Infrastructure Security Agency, or CSISA, at DHS, which would rename and reorganize the National Protection Programs Directorate.

This change reflects the important work we carry out every day to safeguard and secure our election infrastructure.

Thank you and I look forward to your questions.

[The prepared statement of Mr. Masterson was submitted for the record.]

Chairman BLUNT. Well, thank you, Mr. Masterson.

Senator Klobuchar and I plan to stay for both panels and through this one. I am also interested to hear what other peoples' questions are.

There are two areas that Members of the Congress generally, and the senate specifically, think they are experts at: elections and air travel.

[Laughter.]

Chairman BLUNT. You are here for the elections part of that.

We will start with Senator Capito, followed by Senator Cortez Masto.

Senator CAPITO. Thank you, Mr. Chairman, and thank the Ranking Member.

Thank you all for being here with us today.

I would just like to ask a clarifying question. In the past, last year I was the lead appropriator on the FSGG subcommittee, which provided the $380 million to the EAC.

The way I looked at the budget the previous year, 2017, it appeared as though the EAC had a $9 million budget.

Is that correct, Mr. Chairman?

Mr. HICKS. Yes. Our operating budget is about $9 million and so that additional $380 million was just for appropriations to the states.

Senator CAPITO. For the grant. I am going to admit to being a skeptic because I am thinking, "Do you go from $9 million to $380 million? Are they really going to be able to handle this?"

The testimony that I have heard so far, while I have some questions, kind of rests my mind. I want to thank you all for being here today.

Mr. HICKS. I also just want to say that we have given out $3.4 billion over the lifetime of HAVA.

Senator CAPITO. Yes, so you are well versed in this.

I do think, too, our election systems, because of the diversity of the states and local is in some ways, and this may be a bit of a naïve thought, but I do think it does lend us to preserving security. Rather than having a one, singular system all across the Nation that if it got hacked or something would present even greater problems than what we have seen in the past.

I also want to give a shout out to my Secretary of State, Mac Warner. West Virginia has been very much at the forefront of this. We were the first state to get our narrative grant explanation in to you, and we have received the $3.6 million from the appropriation.

Part of what I believe Secretary Warner wants to do, and will be doing with those dollars, and you explained this in your testimony, is to purchase new equipment and update some of the 2004–2005 equipment.

Could you speak to what the increased security is that those systems have now as compared to, say, 12 or 13 years ago?

Mr. HICKS. Yes and no, in terms of being able to talk directly because I am not a computer expert overall. But I would say that our Voluntary Voting System Guidelines, which we are updating now were not updated, have not truly been updated since 2007. Those updates, basically, were before the smart phones, and iPhones, and tablets, and things like that.

Since that time, we have gone technologically far in the future in terms of security and accessibility and so forth with phones and other aspects of computer technology. The EAC has updated our standards for that in terms of voting equipment overall.

New voting equipment that is being tested, once those new Voluntary Voting System Guidelines are approved, once we get a quorum, they will be more stringent, and more accessible, and more resilient for security overall.

Senator CAPITO. Dr. Romine, do you have any thoughts on that topic?

Dr. ROMINE. Nothing specific relating to the actual technologies, but I will say, again, just like Chairman Hicks, we work diligently with the EAC on the development of the new Guidelines, the VVSG to ensure greater emphasis on auditability, on system security, and other things that are critical to the integrity of the elections process.

Senator CAPITO. Let me ask another question and topic that I have great concern on in the urban and rural areas.

Senator Klobuchar and I have worked on this, along with Senator King, I see in the room, on our broadband caucus connectivity. This is sort of an open question for anybody on the panel.

Do you see in the future—and I think Senator Lankford talked about, we know maybe what 2020 is going to look like, but what is 2040 going to look like—do you see some difficulties with certain states that have a lower reach of broadband connectivity being able? How would that affect election security in your opinion? Does anybody have an opinion on that?

Mr. MASTERSON. Thank you, Senator, and I will offer a brief one.

This is, in part, I think, why we run elections locally is that ability to deploy those systems to those polling places in the locality with the local election official and serve the process without a need for that connectivity in that way.

The resource challenges for rural jurisdictions are real and I think the money that Congress appropriated is an important first step in helping support, not just those larger jurisdictions in particular, infuse some money down to the local level to help them take the steps they need to do to improve the results of the process.

Senator CAPITO. Then, my take away from that would be that the EAC has built-in to their parameters a flexibility component depending on what the individual needs are of urban, rural, large, small, whatever those particular needs might be.

Is that a correct statement?

Mr. HICKS. Whatever states need, we are there to give it to them, whether or not that is what works in Maine might not work in West Virginia sort of thing.

I have gone through, since I have been in this position, 39 of the 50 states and every state is the same, but every state is different, whether or not that is the urban areas or the rural areas.

Because one of the misconceptions that I have noticed in this is that elections are not run by these huge jurisdictions in terms of having 10 or 15 people and so forth.

Senator CAPITO. Right.

Mr. HICKS. It is one or two individuals doing more things, basically from my testimony of ADA compliance or even driving a school bus.

Senator CAPITO. Right.

Mr. HICKS. From A to Z.

Senator CAPITO. Thank you.

Thank you, Mr. Chairman. Sorry I went over there a little bit. Thank you.

Chairman BLUNT. Senator Cortez Masto and then Senator King.

Senator CORTEZ MASTO. Thank you, Mr. Chair, and Ranking Member.

Let me followup on the discussion you talked about. Right now, there is not a quorum on the EAC and because there is no quorum, you are unable to pass the Guidelines 2.0.

Is that correct?

Ms. MCCORMICK. That is correct, Senator.

Senator CORTEZ MASTO. How else is a lack of a quorum impacting the work of the EAC?

Ms. MCCORMICK. We are able to do almost all of the work that the EAC staff puts forth. The day to day operations and the support that we can give to the states does not stop.

We are not able to vote on new policy. That is the one area that we are restricted when we do not have a quorum, and that would include the VVSG.

Senator CORTEZ MASTO. Once you do have a quorum, is it ready to be voted on and moved quickly?

Ms. MCCORMICK. It has gone through our Standards Board and our Board of Advisors for their input, and they have voted to approve it. It needs to go out for public comment.

If we do get another commissioner, and hopefully we will, and establish a quorum, I think it will be up to that commissioner to decide whether he or she is comfortable with the approach that we are taking. We will have to socialize what we have done with that commissioner so that we can all be on the same page when it comes time to voting for the new standards.

Senator CORTEZ MASTO. Thank you.

Then, it is my understanding that not every vendor is certified. Is that correct?

Mr. HICKS. Yes, because these are Voluntary Voting System Guidelines.

Senator CORTEZ MASTO. Can I ask? How long does it normally take to certify a vendor?

Mr. HICKS. It could range.

I do not want to fudge the answer, so let me get back with you on that one.

Senator CORTEZ MASTO. If you could, that would be helpful.

[The information referred to was submitted for the record.]

Senator CORTEZ MASTO. I am just curious.

How many actually are certified and how many vendors are not certified that are actually in our states and machines that we are using?

Mr. HICKS. That we?

Senator CORTEZ MASTO. If you could followup with that, that would be helpful.

Mr. HICKS. Right. We can get that information back.

Senator CORTEZ MASTO. Thank you. I appreciate that.

[The information referred to was submitted for the record.]

Senator CORTEZ MASTO. Mr. Masterson, how many states have asked DHS for risk and vulnerability assessments on their election systems? Actually, how many states have received those assessments?

Mr. MASTERSON. Thank you, Senator, for the question.

As it stands now, 18 states have requested. We have performed 17 of those, or have them in process. They are in the process of having our teams deploy out. We have one that we are waiting to schedule.

Senator CORTEZ MASTO. Would you please provide us with a list of those states that have received those assessments? Would that be information that is public, at least, or available for us to know?

Mr. MASTERSON. Senator, I will take your request back to the office.

Senator CORTEZ MASTO. Okay.

Mr. MASTERSON. Generally, we do not share who we work with on any one of these services to preserve the trust and the relationships, so that they will continue to engage with us. But I will go back and pull together what information we can share with you.

Senator CORTEZ MASTO. I appreciate that. Thank you.

Mr. MASTERSON. Yes.

[The information referred to was submitted for the record.]

Senator CORTEZ MASTO. Let me jump back to an issue that also keeps coming up and we just heard it earlier today with the Senators.

There is a lot of discussion about risk-limiting audits and whether or not they should be used more broadly across the country. Let me start with the EAC Commissioners, Mr. Hicks and Ms. McCormick.

Can you describe in more detail the types of audits that are most effective in the process of putting these audits in place and the difference that they may make?

Mr. HICKS. The audits depend on the state and the way that they do their voting.

For instance, a state like Oregon is an all-mail-in ballot state. Doing a risk-limiting audit would be really helpful for them.

A state that does not have a paper audit trail, it is not going to really work so well with them, but there are ways to audit those systems as well. But it just depends on what the states want to do in terms of the way that they want to have their audits run.

We had the pleasure of going out to Colorado recently and witnessed their risk-limiting audit, and it functioned fairly well. I feel that other states are going to be taking that into account, like Rhode Island and New Mexico as well, to see what sort of audits can be done. Audits only work if they are being done.

Senator CORTEZ MASTO. Right.

Mr. HICKS. If states have audits on the books, but they are not conducting them, then that is where the real problem lies.

Senator CORTEZ MASTO. Okay.

Ms. MCCORMICK. I just want to stress that we need to remember that every state does a canvas. The canvases do cover a lot of that.

Some states can do risk-limiting audits, some cannot be based on what kind of systems that they are using. But all the states do some sort of auditing in some form or another.

Senator CORTEZ MASTO. That was my next question.

It is purely voluntary for the states the type of audit that they conduct, but the followup is, to your knowledge, every state is doing some type of audit.

Ms. MCCORMICK. I think every state is doing some type of audit, if not at least a canvas before they can certify an election. I would assume that that would be considered part of an audit if you are going to canvas the election before you certify it.

Senator CORTEZ MASTO. Okay. Thank you.

As my time is up, thank you, Mr. Chair.

Chairman BLUNT. Thank you, Senator.

Senator King.

Senator KING. Thank you, Mr. Chairman.

First, I want to thank you and Senator Klobuchar for calling this important hearing. I think this is a critically important issue and

one that, I am not sure gets enough attention. I am delighted that we are working on this today and that Senator Lankford was here talking about his bill.

Mr. Hicks, this is complicated: decentralized systems, all kinds of voting systems, and machines, and all of that.

Is it safe to say, though, that the simplest rule should be, there should always be a paper back-up?

Mr. HICKS. Senator, thank you for that question.

It depends on the state. We cannot basically regulate.

Senator KING. I am not suggesting regulation. I am making a suggestion. It seems to me this is a basic thing. I am not saying they have to do it, but if you do not have a paper back-up, it is very hard to determine whether you have an accurate count.

Mr. HICKS. Paper is interesting because every one cannot use paper. If you have a disability, you come back from Iraq with no hands, it is hard to do that paper piece of it.

I would say that if we can do security with paper to make sure that it is accessible to those who have disabilities, then I would say that that is one hundred percent right that we should have a paper back-up.

Senator KING. I want to direct a question to Dr. Romine and Mr. Masterson.

I serve on the Intelligence Committee and we spend a lot of time with cyber security issues in the intelligence community. One of the most powerful tools we have is the Red Team and bug bounties.

One of my concerns is that the states are at varying levels of security. I do not want to say they are overconfident, but they have a level of confidence that may not be justified. My old admonition from President Reagan was, "Trust, but verify."

How about a provision that either NIST or Homeland Security could Red Team? Which means, try to penetrate these systems. There would be nothing like having a Secretary of State's computer have a signal come up that says, "Greetings from Washington," to get their attention in terms of what they need to do.

Is that something that you have thought about, because it is used in the intelligence community to great effect. Everybody can feel like they are really protected until somebody shows them they are not. That is what I am suggesting.

Dr. ROMINE. Speaking just from the NIST perspective, however interesting an idea that is, it would be outside the purview of a NIST function. We are not really in the operational mode.

I think we are experts at the development of guidelines, and standards, and providing tools to people. But with regard to Red Teaming, that is not something that would be appropriate for NIST to do.

Ms. MASTERSON. Senator, thanks for the question.

As you are aware, DHS offers a variety of free services to state and local officials, including onsite assessments like risk and vulnerability assessments, which are in-depth, penetration tests of the systems.

States and localities are able to use these services as they see fit. In addition, we offer——

Senator KING. What bothers me in your statement is the word "offered". The ones who are not asking for it may be the ones who need it.

Ms. MASTERSON. Senator, I understand your point. I would also add that our offerings are not the only offerings that states are taking advantage of.

We have seen—as we have gone out, and met, and talked with state and local officials—that state services use the National Guard, as well as private sector partners, are being used in these same ways with the services that we offer.

My experience is that the states are taking this seriously in engaging. Certainly testing, like penetration testing, Red Team testing, is of value and many states are doing that in some way within their jurisdiction.

Senator KING. Do you have an overall assessment of how secure the American voting system is going into 2018, which is now 4 months away?

Mr. MASTERSON. Yes, I have confidence that the process is resilient in that election officials working with us, state resources and localities have the ability to protect based on the resources they have, but also the ability to detect and recover, which is what we talk about frequently.

Senator KING. We are talking pretty much about voting machines and that kind of thing, but I see a real vulnerability is voting lists and the lists that are maintained mostly at the state level.

It would not take much to disrupt an election. Take out everybody who is named "Smith" or something, then people would show up at the polls and could not vote.

Are the registration lists secured?

Mr. MASTERSON. The states have taken numerous steps, depending on the state, to improve the security. Again, it comes back not just to protection—because as you know well, these are sophisticated actors—but the plans that are in place to respond.

Senator KING. That was in my notes, sophisticated actors.

Mr. MASTERSON. Yes, so that ability to respond and recover. In Federal law, with your example of registration lists, that ability to have that provisional ballot for all voters who believe they should be on the list and they are not, that is an important piece of resilience in the elections process that everyone can receive a ballot regardless if they show up and are told they are not on the list.

Senator KING. I am over my time, but the provisional ballots, are those provisioned in every state?

Mr. MASTERSON. That is Federal law. Yes, sir.

Senator KING. That is mandated.

Mr. MASTERSON. Yes.

Senator KING. Thank you very much.

Mr. MASTERSON. Thank you, Senator.

Senator KING. Thank you, Mr. Chairman.

Chairman BLUNT. All right.

Before I go to Senator Udall, I would maybe ask our next panel if they can begin to think about how their 5 minute opening statement could be more like 3 minutes.

As you think about that, we do have votes at noon. We will be able to work through part of that after 12 o'clock time, but we do

want to get to you and the rest of us want to ask this panel questions.

Senator Udall, it is your time.

Senator UDALL. Thank you, Chairman Blunt.

Mr. Masterson, I guess to you, and Mr. Hicks, and Christy McCormick, what are your agencies doing to further post-election audits in every state?

Mr. MASTERSON. We worked with our Government Coordinating Council that created funding considerations. Considerations for the use of the HAVA funds that Congress appropriated.

Included in those is stressing the importance of post-election auditing and the need to conduct post-election audits. We are continuing to work with the Government Coordinating Council on those practices.

Senator UDALL. Ms. McCormick.

Ms. MCCORMICK. Yes, we provided a lot of information to the states on how they could use the HAVA funds, and post-election audits were included in ways that they could use that money. We will provide guidance in that regard, if the states choose to use their money in that way.

Senator UDALL. Yes.

Mr. HICKS. The same.

Senator UDALL. Yes. Are states working well with the Election Assistance Commission and the Department of Homeland Security to ensure ample communication and sharing of resources to ensure elections are secure? What can be done to improve communication with the states?

Mr. HICKS. We are working a lot better than we did in 2016. With the formation of the Government Coordinating Council, and working with DHS and the FBI, we are functioning a lot better at this point than we were two years ago during that election season.

Senator UDALL. Great, thank you.

Chairman Blunt, recognizing we will have another panel here and we have votes, I am going to yield back at this point, so you can get going.

Chairman BLUNT. Well, thank you, Senator.

Senator Klobuchar.

Senator KLOBUCHAR. Thank you very much, Mr. Chairman.

Mr. Masterson, there have been statements indicating that foreign adversaries do not pose a serious threat to our elections. I am sure you are aware of that.

Some people have been saying things, but you also know that all of our security heads in this country, under both President Obama and now President Trump, have stated that this firmly has happened and that it is a threat moving forward.

I think it was former Senator Coats, who is the National Intelligence Director, who has said that, in fact, they are getting bolder.

Can you confirm that the threat against our election system is real and the work that state and Federal officials are doing to update and secure our elections is warranted?

Mr. MASTERSON. Senator, thank you for your question.

As I said in my opening comments, elections are a target. There are real risks to the election systems. Whether or not there are specific threats targeting election infrastructure is irrelevant to the

importance of the information that we share with state and local officials to continue to build the resilience and overall cyber security of the process.

Our focus remains on helping states identify and mitigate those risks, and that work is important.

Senator KLOBUCHAR. Commissioner Hicks, several of the election officials at our last hearing complimented the EAC's efforts to quickly distribute the $380 million for election security funding from March.

According to your testimony, in just over 3 months, the EAC has received disbursement requests for 97 percent of the funds from 51 of the 55 states and territories. I have seen some reporting that indicated delays.

Can you explain these varying accounts very briefly?

Mr. HICKS. Some of the delays have just been associated with legislation, so basically, the chief election official having to go back to their legislatures to figure out how to request that money.

Senator KLOBUCHAR. You mean like in my state?

Mr. HICKS. I did not want to say it.

[Laughter.]

Senator KLOBUCHAR. Yes, not the fault of our election person. All right, very good.

Dr. Romine, according to requirements in the Help Americans Vote Act of 2002, with the current configuration, there should be four technical experts on the Technical Guidelines Development Committee.

How many of these technical experts are cyber security experts?

Dr. ROMINE. I will have to get back to you on that. I do not know that off the top of my head.

Senator KLOBUCHAR. Okay.

[The information referred to was submitted for the record.]

Senator KLOBUCHAR. Well, as you may know, Senator Lankford and I, our bill would expand the Technical Guidelines Development Committee's mission and membership to provide additional cyber security expertise.

With this expansion, do you think the new and improved committee would be better equipped to provide best practices and recommendations in election cyber security?

Dr. ROMINE. I think additional expertise in cyber security would be welcomed in almost every facet of anything we do.

Senator KLOBUCHAR. Okay. Then finally, this is building on to what Senator Cortez Masto was asking about, but the Secure Elections Act calls for states to implement audits in order to confirm election results.

Do you believe—and anyone can take this—that performing a post-election audit is a best practice that should be used to increase confidence in the outcome of Federal elections?

Mr. HICKS. Yes.

Senator KLOBUCHAR. Do you all agree?

[Panel nods assent.]

Senator KLOBUCHAR. Very good. May the record reflect they all nodded their heads yes. All right. Thank you.

Chairman BLUNT. Thank you, Senator.

I will ask a couple of questions while Senator Warner is thinking about how he would like to close these questions out.

There will be a time to submit written questions, and there will be written questions.

Commissioner Hicks, the $380 million that was allocated to the states through you, how much of that is now out the door? How much of that is on the way to states?

Mr. HICKS. Ninety-seven percent has been requested and we usually get it out within less than a week being allocated out. I can get the exact number of the dollar amount during our written.

Chairman BLUNT. I thought it was mostly gone by now. I know $154 million was out within the first 30 days or so.

Mr. HICKS. It is more than $200 million.

Chairman BLUNT. You are almost totally out now.

Now the states, there are no required standards they have to meet to qualify for that money currently?

Mr. HICKS. There are requirements that they have to meet under HAVA, under the law.

Chairman BLUNT. But things like having an auditable ballot trail would not be one of those requirements.

Mr. HICKS. Correct.

Chairman BLUNT. You mentioned that in a non-paper environment, there were ways to audit the returns. I am trying to come up with what one of those ways might be that, with certainty, would guarantee that what happened on election day was what happened.

How would you audit those non-paper systems?

Mr. HICKS. They are audited because there are really no non-paper systems. It is more of a physical paper ballot that people are testifying to.

Each system has a paper record incorporated in its system which is encrypted and so forth. That is where the auditability comes.

Chairman BLUNT. They would look at the paper record that was generated by the individual voting device?

Mr. HICKS. Right. The issue becomes whether or not that is a voter verified paper record with the auditability.

Chairman BLUNT. I understand.

Commissioner McCormick, you said that the canvas might be the audit. The canvas is really where local officials report to state officials what their final county return is. Right?

Ms. MCCORMICK. Right. They check over all of the paper trails from the machines, all the paper receipts and make sure that the machines match all the numbers. In a way, those are audited numbers before that they are certified. Election night reporting is not official.

Chairman BLUNT. Right.

Ms. MCCORMICK. It has to go through a process where they check all of the paper receipts and check all of the voting numbers against those receipts to make sure that they can certify it as official results.

It is not exactly an audit, but it is a form of an audit.

Chairman BLUNT. I think it is not exactly an audit, but I understand what you are saying. Election night returns are always unofficial.

Ms. MCCORMICK. Correct.

Chairman BLUNT. Always need to be verified. On that topic, let me go to one other.

I think in the Maryland primary that was just completed, some of the registrations were not downloaded appropriately. I do not know how many provisional ballots were cast because of that.

Do either of you know?

Ms. MCCORMICK. I do not know the numbers. We can get that from Maryland for you.

Chairman BLUNT. No. I think we are in the process of getting that.

One of the things I wonder about there, we have had a lot of concern about what happens if the Election Day record is not what you would want it to be, which is exactly what happened in Maryland.

I think my two questions on that would be how much does it slow down the Election Day voting process, if you have to cast that provisional ballot? Maryland may be one of the examples of most of those ballots cast in recent times.

Another question that I would have—and I am just letting you know my interest in this—is how much that then slowed down the final results?

Every state does have, as you have pointed out, a provisional ballot requirement if a voter shows up and, to make the case that they should be allowed to vote in their name, for whatever reason is not on. It at least applies to all Federal elections.

Is that right?

Ms. MCCORMICK. Yes, that is a requirement under HAVA.

Chairman BLUNT. Right.

Ms. MCCORMICK. All states have to have provisional ballots.

There have been a number of cases recently where, I think Los Angeles was also a jurisdiction recently that had names left off of their voter registration lists and probably used provisional ballots as well.

They do add some time. They can create lines and I think that is one of the concerns with any possible attacks on voter registration systems as well because if there were, we would have to rely on provisional ballots to assure that those voters were actually registered and eligible to vote in an election.

That could cause some delay, but a lot of the voter registrars across the country have that process down quite well, and they do a lot of training with their election officials on how to do that.

Chairman BLUNT. Right.

Senator Warner and then Senator Wicker.

Senator WARNER. Thank you, Mr. Chairman.

I want to thank you and the ranking member for holding this hearing, and the very good work that you have done on this subject matter. As you know, it is something that those of us, who share a common position on the Intelligence Committee, have also bought a perspective to it.

I appreciate all of the panel being here.

I really want to give two questions because I know we have a second panel coming up. I thank the leadership of the committee for getting that $380 million into the budget to try to help assist election officials around the country.

I have a two-part question. The first part is it is hard for any enterprise, even large enterprises to evaluate, I think, the cyber security claims that firms make in terms of what kind of protections that they are going to put in place.

Does the EAC give any guidance or kind of best practices as individual states or localities start to evaluate the effectiveness of some of the cyber security protection monitoring that is being offered out in the marketplace?

Mr. HICKS. We do not give that sort of specific advice, but we have worked with DHS to say that these are some of the things that are free that are available to you, like monitors and so forth.

Individual election officials have to be vigilant in terms of knowing that there are going to be pop ups out there who are just going to be looking for a quick buck, to earn a quick buck.

But I believe that the way that the EAC has done now in providing resources to the states, in terms of things like IT management for election officials, has helped them. Basically giving them other aspects, and providing videos to them, and so forth allows them to have a little more confidence in the way the systems work.

Senator WARNER. Are there any independent rating entities?

Again, we have a lot of the cyber security firms located in my state. I applaud all of them. But boy, sorting through who can actually produce is a tough, tough challenge.

I think for election officials in an enterprise that this is not their specific expertise domain would be a real challenge. As you answer that, let me get to the second part of my question, since my time is running down.

From the intelligence side, and I think we just saw in 2016 the tip of the spear of the ability for social media entities, and others, to manipulate information.

One of the questions I have is, and I think maybe Colorado has actually thought about this, is as you think about election monitoring, are any states actually looking at evaluating how some of the social media platforms may be communicating, or miscommunicating to voters within your states? Could some of the HAVA funds be used to acquire that expertise?

Mr. HICKS. I would say that this is nothing new in terms of the misinformation being put out. It used to be that the information would be on posters, "Republicans vote on Wednesday, democrats vote on Thursday." Now it is a lot quicker through social media.

Senator WARNER. But now you can touch a whole universe or the world with a keystroke.

Mr. HICKS. Correct. We, at the EAC, we have met with some of the technology groups, those informational social media groups to find out some of the things that they are doing to ensure that this does not happen again or ways to prevent it.

They have given us some assurances of things that they put in place with this, but I do not believe that the HAVA funds overall can be used toward that. I can go back and check with our grants department because it is very broad on what you can use that money for.

I would think if you are looking to improve the process of the election overall, the administration of elections, you should be able

to use that money, but I want to make sure of that before I give you a definitive answer.

Ms. MCCORMICK. I will just add that we are encouraging state and local election officials to monitor their social media to make sure that correct information is out there. If they see something that is incorrect to contact the platform and make sure that it is taken down or corrected.

Senator WARNER. I would hope that there might be some way and I think the social media companies have been slow. They are getting better at responding, but there needs to be some level of ongoing communication and collaboration.

I hope we could work with the committee to see how we might work on that.

Thank you, Mr. Chairman, and it is great to attend a hearing with you and such a distinguished ranking member.

Chairman BLUNT. Thank you, Senator Warner.

Senator Wicker.

Senator WICKER. Mr. Chairman, in light of the fact that we have another panel, I will wait.

Chairman BLUNT. Thank you, Senator Wicker.

Senator Cruz.

Senator CRUZ. Thank you, Mr. Chairman.

Thank you to each of the witnesses for being here, for your testimony.

Mr. Masterson, in 2017, the Department of Homeland Security declared state election systems to be critical infrastructure.

Can you discuss what the practical effects are of this designation and what DHS has done differently since that designation with regard to state election systems?

Mr. MASTERSON. Yes, thank you, Senator, for the question.

The focus of our work in declaring elections as part of critical infrastructure is threefold.

One is ensuring that state and local election officials have access to timely information shared with them such that they can mitigate risks that arise to their system. This is largely done through our Information Sharing and Analysis Center of which all 50 states are members.

We routinely share information out through the Information Sharing and Analysis Center to ensure election officials have the information they need, whether general or technical to protect their systems.

Second is providing services to those state and local officials on a voluntary basis. We provide onsite risk and vulnerability assessments, remote cyber hygiene scans, assessments on resilience readiness in order to help support those state and local officials, should they need it.

The third is working at the Federal level with the intelligence community to ensure that intelligence is shared in a timely and actual manner.

One of the lessons I think we all learned from 2016 is to ensure that the system owners and operators, those in charge of elections, are empowered through receiving information and intelligence to protect their systems. We have been coordinating with the intel-

ligence community across the Federal Government to ensure that that information is shared.

Senator CRUZ. In March, Congress allocated $380 million of new spending to be put toward election security.

How is that money being spent? What sort of oversight controls are there to make sure the money is actually being put to good use helping make elections more secure?

Mr. MASTERSON. I will defer to my colleagues on the EAC.

Ms. MCCORMICK. Yes, we have run that money through our grants division in the Election Assistance Commission.

Most of the money is being used for cyber security efforts and for upgrading voting systems, especially the ones that are quite old.

We are requesting all of the states, requiring of all the states to provide a narrative and budget, along with their drawdown of that money, and we will be auditing how that money is used. Every state will be audited on their use of the money and whether it was used appropriately.

Senator CRUZ. How significantly do you assess the threat of an election being directly hacked in terms of the results at the ballot being altered electronically?

Ms. MCCORMICK. I would say that, Senator, it would be very, very difficult to do that given the dispersed character of our election infrastructure.

We have 8,000 jurisdictions. None of the machines are connected to each other, so each machine would have to be hacked individually and that is one of the greatest securities that our election system actually has. It would be extremely difficult to do that.

That said, every system is vulnerable and things can happen, but election officials are extremely vigilant.

We do logic and accuracy testing on every single machine before it is used in an election that is open to the public, so we can check to see that the machines are actually recording the votes correctly. There are numerous ways to check it afterwards. We discussed earlier some post-election audits.

It would be very hard to do that. However, I cannot ever say "impossible".

Senator CRUZ. Am I correct, there has obviously been a lot of discussion about 2016, but am I right that there are no indications that there was any actual hacking of election equipment that altered outcomes?

Ms. MCCORMICK. We do not know of any outcome that was hacked or changed in any way. What happened in 2016 has been characterized by Undersecretary Krebs as overstated and that it was mostly drive-bys and scans.

We actually see thousands and thousands of these types of scans every single day across the Nation against every single system. I would say that we are concerned about security of the system, of the entire election system.

Nothing happened in 2016, and that is the real untold story that the election officials did their job, and they kept system safe from any sort of hacking.

Senator CRUZ. What would you characterize as the most important security reform that state election authorities should put in place to ensure the integrity of the ballot process?

Mr. HICKS. I would say that we need to make sure that the confidence of the voter remains high because if we erode that confidence, the voters are not going to come out and actually cast their ballots.

I think from A to Z, basically from voter registration all the way to election night reporting, all those points are valid and important.

Senator CRUZ. Thank you.

Chairman BLUNT. Thank you, Senator Cruz.

Thanks to the panel.

At some point, I know one of my followups will be if you are having these thousands of attempts to get into systems all the time, what do we do and how do we help local and state election officials figure out which of those they need to take seriously?

I think we had one group of state officials here last week and one of those state officials said they had 100,000 attempts in, I believe he said, every day to get into their system. If they report 100,000 attempts to you, I do not know what you do about that, but that will come in writing.

Let us move to our second panel. Thank you all for being here. Obviously, very great interest to the country and the panel, and we are grateful that you were here.

On our second panel, Mr. Scott Leiendecker is the CEO of KNOWiNK. It is a company that provides the iPad registration booklets in more than half the states now, I believe, including the District of Columbia.

Mr. Peter Lichtenheld is the Vice President of Operations of Hart InterCivic.

Bryan Finney is the CEO and Founder of Democracy Live. He is representing the Sector Coordinating Council.

We have moved from the government part of the hearing to the nongovernment part of the hearing. We will see how this goes, but we are glad to have you here.

We have your written testimony. It is part of the record. Mr. Leiendecker, if you want to start by either reading or summarizing what that testimony has told us before we get a chance to ask you a couple of questions, that would be fine.

OPENING STATEMENT OF SCOTT LEIENDECKER, CEO, KNOWINK, ST. LOUIS, MISSOURI

Mr. LEIENDECKER. Thank you, Senator Blunt, Ranking Member Klobuchar, and members of the committee.

Thank you for today's opportunity to be with you. I am grateful for your willingness to engage and take into consideration the vendor's perspective.

What I was here to talk about specifically is my experience in the past as a former election director. I think that is a unique perspective that I can bring to the table.

I want to talk about the different things that we do to ultimately secure our products, which is our electronic poll roster that basically uses the iPad that ultimately helps with the security side and leverages the security of the iOS operating system.

To kind of sum up very quickly, in order to continue innovating and providing strong security initiatives, we hope that the Federal Government will consider us a partner. We hope that today's hear-

ing is just the beginning of a new conversation with the committee and the Federal Government will have with election vendors.

Together with the local election vendors—like the ones in Missouri and in Minnesota that are on the frontlines in today's elections and throughout the election process—we want to offer this committee, and others in Federal Government, our assistance to help shape that public policy and ensure the integrity of our most secure process.

Thank you.

[The prepared statement of Mr. Leiendecker was submitted for the record.]

Chairman BLUNT. Mr. Lichtenheld.

OPENING STATEMENT OF PETER LICHTENHELD, VICE PRESIDENT OF OPERATIONS, HART INTERCIVIC, AUSTIN, TEXAS

Mr. LICHTENHELD. Thank you, I will keep my comments short, as I know we are running short on time. My name is Peter Lichtenheld.

Chairman Blunt and Ranking Member Klobuchar, thanks for having us here. committee members, thank you.

I am the vice president of Operations with Hart InterCivic. We are a voting system provider based in Austin, Texas. We serve about 27 million voters across the United States of America and we are part of the solution on election security working with DHS, the EAC, and other bodies, and as members of the Sector Coordinating Council.

I want to clarify that voting systems are not just commodities, but solutions and that we are partners with our customers. We are constantly working with customers. We do not just sell them something and then expect them to run it on their own. We are constantly sharing best practices with customers, doing Webinars, giving papers to customers, and helping them run secure elections.

I also want to go off my written record for a minute and talk about Senator Wyden's comments and address those specifically because Hart InterCivic is an important voting system provider in the United States. We have been open. We do not stonewall.

We did open and answer the letter that Senator Wyden sent to voting system providers, and our core values at Hart are about candor, which I am using right now and about integrity, which we feel is very important. Really, one of our basic tenets is that we are election geeks. We love elections and we feel like we are helping America vote.

Thank you.

[The prepared statement of Mr. Lichtenheld was submitted for the record.]

Chairman BLUNT. Mr. Finney.

OPENING STATEMENT OF BRYAN FINNEY, PRESIDENT AND FOUNDER, DEMOCRACY LIVE, INC., SEATTLE, WASHINGTON; SECTOR COORDINATING COUNCIL FOR THE ELECTION INFRASTRUCTURE SUBSECTOR, U.S. DEPARTMENT OF HOMELAND SECURITY, WASHINGTON, D.C.

Mr. FINNEY. Mr. Chairman, Ranking Member Klobuchar, and members of the committee.

I am here today as the CEO of Democracy Live, a Seattle based voting technology firm delivering electronic balloting to members of our military, overseas voters, and the 35 million blind and disabled voters in the United States. That includes the military and overseas voters, Mr. Chairman, in your state on a statewide basis and Senator Warner in your state.

I recently had the honor of being nominated and selected as a founding member of the Homeland Security Elections Sector Executive Committee. This DHS Sector Committee represents a broad and diverse coalition of more than two dozen companies and nonprofits developing, deploying, and supporting elections and voting solutions to meet the needs of our Nation's 200 million eligible voters and the thousands of hardworking elections administrators across the United States.

In addition, our members are working collaboratively with the U.S. Elections Assistance Commission, as well as state and local election offices to ensure secure, stable, and scalable voting systems. The SCC, representing the greater elections and voting systems providers in the United States, absolutely supports the increased focus and attention on the security of our Nation's election systems.

As we know, foreign attempts to probe government voter information platforms during the Presidential campaign were clearly aimed at undermining faith in America's democratic institutions.

While the consensus among the intelligence community remains clear that no vote tallies were altered in any way—and there is no hard, proven evidence that any private sector provider was compromised—the existence of foreign threats means that we need to continue to be extremely diligent in protecting our Nation's critical voting infrastructure and instilling confidence in our U.S. electoral systems.

The SCC members are prepared to meet the threats and challenges that exist. However, with less than two dozen providers serving the needs of over 6,000 elections localities, representing over 200 million voters, expectations must be aligned.

First, existing levels of government investment must correspond and increase to meet the growing threats to the entire electoral system.

As the inventors, innovators, providers, and partners to what is truly the engine of our democracy, it is critical that we are engaged at the start of any strategic planning, testing, educating or other security initiatives relating to voting systems.

As this committee considers how to better secure our Nation's election infrastructure, I would encourage your members to remember that the voting and tabulation systems, although they get the lion's share of the attention, is only the endpoint of a long process with potentially hundreds of voter touch points before that voter even casts a ballot. These touch points must also be secured.

They include items like voter registration, poll books, election night reporting, mail balloting, which is the fastest growing method of voting, and information about who and what is appearing on your ballot.

Finally, laws and certifications exist that can, and should, be strengthened to better secure our voting and tabulation systems,

but if the information systems are corrupted or manipulated, then all the work and resources we put into hardening our voting systems may, in the end, be negated.

In this era of voter bots and social misinformation, more and more voters are turning to their local elections officials for accurate objective information. As it was information systems that were manipulated in the recent Presidential election and not tabulation systems, I would encourage Congress to materially support elections officials to offer secure, objective and accessible voter information that voters can trust.

Thank you.

[The prepared statement of Mr. Finney was submitted for the record.]

Chairman BLUNT. Thank you.

Mr. Leiendecker, you provide the iPad poll book in how many states?

Mr. LEIENDECKER. Currently, we have Poll Pad, which is the iPad-based solution. We are in 25 states, 600 jurisdictions nationwide.

Chairman BLUNT. In Canada?

Mr. LEIENDECKER. Canada just recently acquired our solution.

We actually—just so you know and I think this is some good information—we went through the Ministry of Defense. They did an audit on our solution. The results were just released yesterday and there were zero vulnerabilities in our source code, which was nice to see.

Chairman BLUNT. Could we get a copy of that?

Mr. LEIENDECKER. As soon as I get a copy of it, I could provide that for you.

Chairman BLUNT. Good.

[The information referred to was submitted for the record.]

Chairman BLUNT. I think Senator Klobuchar would want to know this. You are now transitioning a number of Minnesota counties.

Is that right?

Mr. LEIENDECKER. A number of Minnesota counties. We have been working with Secretary Simon in Hennepin County. They have been using our products for about two years now; close to two years.

I think in the primary elections coming up in August 15 or 16, I believe, we will be——

Senator KLOBUCHAR. The 14th.

Mr. LEIENDECKER. The 14th.

Senator KLOBUCHAR. Not that I would know that.

[Laughter.]

Mr. LEIENDECKER. I will be there and a number of us will also be there, but we have about 50 counties that will be moving toward that solution.

Chairman BLUNT. How many voters do you think were included in the registration material you were managing in the last election cycle in 2016?

Mr. LEIENDECKER. 2016.

Chairman BLUNT. This is just an estimate.

Mr. LEIENDECKER. It would be several million.

Chairman BLUNT. Where I am really going here is this question of how many people try to get into these systems and what do you do to determine the vulnerability of the systems that your company works with?

Mr. LEIENDECKER. There are a number of things that we do. From our knowledge, nobody tried to tamper with our product.

One of the nice things about using the iPad is the baked-in security that is already offered. That is one of the things that I really liked about this solution when I was a former director in St. Louis looking at the different solutions available to me.

The baked-in security is a big thing, so I do not have to be a security expert. I am leveraging what is the Apple iPad, which is secured by NIST, and has all the bells and whistles that NIST offers, the FIPS 140–2, all of that.

We leverage security from the security experts. We are not trying to be security experts at our organization, although we do have individuals who are security experts on staff. That is a big part of it is leveraging the right type of hardware and software.

The other thing that we do is obviously encrypt everything on the iPad, so anything that is in transit is encrypted. That is a big part of what we try to do to make sure that we are responsible and thoughtful throughout the process with regard to security.

Chairman BLUNT. Does anybody in your organization try to find the weaknesses in any system that you are trying to manage?

Mr. LEIENDECKER. Absolutely. After we get done testing the application, such as the one in Minnesota that we just got finished with a few months ago, it goes through a number of tests, whether it is internal, that is the first course where we go through and do our own testing. Then ultimately, we send it through penetration tests.

That is a big thing that we have been doing since day one. This was not something that we just decided to do because the Russians decided to try to meddle in our elections process this past election.

This is something that we did from day one to make sure that we were being responsible to our clients. Our clients are provided that information once those penetration tests are done, especially before major elections.

But we have actually started to do more penetration tests throughout the year just because we know that it is important. It is something that is on everybody's mind. We want to be responsible and thoughtful for the product.

Chairman BLUNT. If somebody was monitoring the people trying to get into their voter registration system, part of that could be a legitimate effort on your part to see if it was possible to get in.

Mr. LEIENDECKER. We do not deal directly with the voter registration system.

Chairman BLUNT. Got it.

Mr. LEIENDECKER. We are just, I would say, the poll book, the paper poll book.

Chairman BLUNT. What would your penetration effort be?

Mr. LEIENDECKER. The only concern that I could see is there are jurisdictions that do like to connect these devices in, like a vote center scenario, where the information can move from one area to

the other, to one polling location to the other to make sure that that individual is checked off of the list.

Now, the application is local and it is up to the jurisdiction to so choose if they want to do that, but that would be the only way.

But again, all of that data is encrypted.

Chairman BLUNT. Okay, thank you.

Senator Klobuchar.

Senator KLOBUCHAR. Senator Cortez Masto.

Senator CORTEZ MASTO. Thank you and I know we under a deadline, so I will be quick.

I was talking with the Secretary of State's office in the State of Nevada, and one of the things they brought to my attention, as we talked a little bit about the risk-limiting audits.

But I also understand that the risk-limiting audits and other sophisticated post-election audits require a voting system that can produce what is known as a Cast Vote Record, which is basically an identifier for that ballot. Many of the new voting systems have this capability, but lots of states are still using the older systems that do not produce a Cast Vote Record.

The new HAVA funds are not enough for all the states to purchase all of the newer voting systems.

Is there anything that you, as vendors, are doing to support expansion and upgrades of risk-limiting audits and other sophisticated post-election audit processes?

Mr. LICHTENHELD. Yes, I will answer that one.

We do have a new voting system at Hart. We started developing that voting system in 2015. It is new from the ground up, so it takes advantage of all of the new security features. The first person we hired to help us build that was a security officer and it does support risk-limiting audits.

We have customers who have risk-limiting audits required in their states or as optional in their states. We do encourage that every state have some sort of audit and that a lot of thought be put into risk-limiting audits.

Senator CORTEZ MASTO. Any other comments?

Mr. FINNEY. As an executive member of the Executive Committee at the Homeland Security Coordinating Council, I would say that the emerging technologies, almost all of them will provide some of either a voter verified paper trail or a cast ballot record.

Senator CORTEZ MASTO. Okay, thank you.

Then just one final thing, you heard the previous discussion on certifying the machines. That is purely voluntary. My understanding, after talking with some of the folks in the State of Nevada, the reason why some of them do not go through that process is because it is cumbersome. That is what I am told.

Is that right?

Mr. LICHTENHELD. That is correct.

Senator CORTEZ MASTO. Okay.

Mr. LICHTENHELD. I am glad you brought that up. I took note of your question about that. Different voting system providers have different approaches to that, so I can only speak for my company.

At Hart InterCivic, what we do is we always go through the EAC because it is a trusted method of having your system tested by an

independent testing lab, and then having a stamp of approval from the Federal Government before you go to the states.

Not all states require an EAC certification, but most states require at least a voting system testing lab, and that lab for most states has to be approved by the EAC. What we figure is why not go through the other step of having it EAC approved?

Senator CORTEZ MASTO. Right.

Mr. LICHTENHELD. Everyone then has a feeling of confidence in that. A lot of this is about voter confidence. We want voters to be confident that their votes count and that they have faith in the franchise.

Senator CORTEZ MASTO. I appreciate that and I agree with you.

But is there a reason why some are not going through that process? Should we be looking at that? Is it cumbersome? Is it slow? Is it too expensive? I do not know. Should we be looking at it to make sure everybody goes through that process?

Mr. LICHTENHELD. Yes, yes, and yes. I cannot speak for the other companies. It is cumbersome. It is sometimes slow and it is expensive, and we do not always agree with the interpretations of the written VVSG.

Senator CORTEZ MASTO. Okay.

Mr. LEIENDECKER. Senator, again, I would just caution that the voting machines themselves are only one element of the entire electoral process.

You can harden the machines. You can have a Cast Ballot Record. You can have the audit. You can have the voter verified paper trail.

But again, if the way that we are either registering to vote, if we know how to vote because of maybe corrupted sample ballots, or other information from social media is manipulated, then at the end of the process, no matter how secure that tabulation system was, if the information was manipulated going to the voter, that perhaps is an even larger concern.

Senator CORTEZ MASTO. Thank you.

Thank you, Mr. Chair.

Chairman BLUNT. Senator Klobuchar.

Senator KLOBUCHAR. Very good.

From your testimony, I know you were all taking this threat seriously. I was pleased Senator Shaheen and I wrote a letter asking if any of the top three voting machine companies have been asked to share the source code or other sensitive details with Russian entities. I was very pleased to receive a prompt response that that had not happened.

But I just need to know very clearly on the record whether you acknowledge that your company, and companies like yours, may be a target for foreign adversaries seeking to disrupt our elections. This does not mean that you have been or that they have gotten through, but you could be a target.

Mr. LICHTENHELD. We are very aware of that and we are very diligent about defending against that.

Senator KLOBUCHAR. Okay.

Mr. LEIENDECKER. Yes, that is accurate.

Mr. FINNEY. We take that very seriously and we believe that part of our job is to protect the engine of our democracy, which are the voting systems and the voter information.

Senator KLOBUCHAR. We have heard that election officials are often limited in their ability to fully assess their cyber security vulnerabilities because of vendor contracts.

Do your contracts restrict election officials from conducting third party vulnerability assessments?

Mr. LEIENDECKER. With our system? No. It allows them to do it and we would work with them to do so.

Senator KLOBUCHAR. Okay.

Mr. LICHTENHELD. Our contracts do not prevent a customer from doing that. We would like customers to let us know if they are doing that.

Senator KLOBUCHAR. That would be nice, yes. Okay.

Mr. Finney.

Mr. FINNEY. We, in fact, embrace that. We encourage that.

Senator KLOBUCHAR. Do you think it is responsible to sell paperless election systems in 2018, given what we know?

Mr. LEIENDECKER. To sell paperless voting systems?

Senator KLOBUCHAR. Yes, with no paper back-up.

Mr. LEIENDECKER. My experience, just as a former election director, I do not see a reason not to. I think it is responsible to have a paper attachment to it.

I understand some of the concerns that Chairman Hicks had brought up, but I think that there are things in place with the Help America Vote Act that secures that. But I do not see why there would not be.

Mr. LICHTENHELD. We at Hart, we support local choice. If local choice is for a paperless voting system, then we do provide that and it is based on state certification guidelines.

There are, I want to make clear, there are Cast Vote Records on electronic voting systems and electronic voting systems can be audited. There are redundant copies of the Cast Vote Record and they can be compared against each other for audits.

Mr. FINNEY. I would caution the Congress to always think about paper as the panacea in part because of the 35 million blind and disabled voters.

Perhaps they cannot see the ballot. They have a reading challenge. They have literacy issues. They have visual impairments coming back from Iraq and Afghanistan. They are blind.

There are innovations that are taking place, the State of Washington, as an example. The State of California developed and is deploying accessible audio capabilities.

For things like my home State of Washington, where it is 100 percent paper, that is wonderful for most of us in this room here today because we can see the ballot. But if you cannot see the ballot because you are blind or visually impaired, what can you do about that?

We have to leave room for innovations and accessibility.

Senator KLOBUCHAR. Thank you.

How do you communicate with your customers about security concerns? Do your contracts generally contain language that clearly

establishes responsibilities for notification of cyber security incidents or vulnerabilities?

Mr. LEIENDECKER. How we communicate is typically before elections, we work with the jurisdiction, as I spoke earlier. We have done penetration tests.

We help them better understand what we have done. We also give them talking points if there are concerns that they can provide to outside sources like media and things like that.

We have been doing this for some time. This has been done not just in response to the past election, but this has been something that we have been doing almost since day one with our jurisdictions.

Senator KLOBUCHAR. Last August, we heard about 1.8 million in Chicago voter records and potentially sensitive information was being exposed.

The "Los Angeles Times" reporting on the incident, explained that the data were exposed by the city's poll book vendor, which had placed on an Amazon Web Service server a back-up file containing information on every voter in the city.

Mr. Leiendecker, does your company store voter registration data in Amazon Cloud Services?

Mr. LEIENDECKER. We do store data in Amazon's Dev Cloud that is protected, and has the FIPS protection, and everything like that.

The incident that happened in Chicago was a mistake by that vendor. It was not us. But from my knowledge in what they——

Senator KLOBUCHAR. Because of the portion of the cloud they put it on?

Mr. LEIENDECKER. It was not due to the portion of the cloud. They just did not apply a password and they left it wide open, from my knowledge.

Senator KLOBUCHAR. Okay.

Mr. LEIENDECKER. That is what I would consider a stupid mistake.

Senator KLOBUCHAR. Okay, well, that is very blunt. We appreciate that. Thank you.

Mr. LEIENDECKER. Thank you.

Senator KLOBUCHAR. I think Senator Warner has returned.

Chairman BLUNT. Did you really say that was very blunt?

Senator KLOBUCHAR. I said it was, yes. It was blunt. That was my little segue to Senator Warner.

Chairman BLUNT. That is a good thing, though.

Senator KLOBUCHAR. Yes.

Chairman BLUNT. Senator Warner.

Senator WARNER. Very efficient committee and I wish all committees worked this efficiently.

First of all, I will make a generalized comment. I am very concerned that there is a lot of chest thumping about how well we did in 2016.

I think we should be very cautious in terms of some of the claims that have been made and the ongoing threat. An ongoing threat that has been confirmed by every member of the Trump intelligence community that Russia and/or others will be back in terms of trying to penetrate our systems.

Second, I was a businessman longer than I have been in politics. I believe in competition. But it worries me when you have three vendors that control over 90 percent of the market for our voting systems.

I have to take exception following some of the comments that Senator Wyden has made, but I have to take exception to your opening comments, because I can tell you the Commonwealth of Virginia, after the 2016 elections, did an extraordinarily thorough review. I pushed that review. I pushed to make sure that we would have that paper audit trail because we had statewide elections in 2017.

During that time, the 2017 elections, many of our local voting systems elected to turn over their machines to the state when we were that close to the election.

You are one of our vendors. Yet, your company refused to work with the Commonwealth of Virginia in making that equipment available.

The comment that you are transparent and the comment that you are willing to work with all these systems was not the case in the Commonwealth of Virginia.

On a going forward basis, I would like to get a commitment from you that you will work not only with the Commonwealth Virginia, but with other states that are doing such a review. That we are also going to be willing to look at a second half of this problem, which is vendor lock-in.

One of the things we know about IT systems is once you sign that contract, you have that ongoing maintenance contract that oftentimes means—even if a state wants to choose a different servicer—they are not able to do that.

I would like to get a commitment from you that you are, one, willing to work with the Commonwealth of Virginia on a going forward basis and other states.

Two, what you and Mr. Finney, what you are doing, what your systems are doing about moving toward interoperability.

Three, how do we make sure, in terms of third party servicing contracts, that your existing contracts do not preclude that so that you can get fresh eyes.

My fear is by precluding third party servicing, you have that lock-in where a system then does not have the ability to even bring in a third party researcher or others to look at your systems.

Mr. LICHTENHELD. Yes, I will answer all of those questions, sir, or comments.

First of all, yes, I make that commitment to the Commonwealth of Virginia. At that time, we only had a few customers in Virginia and all of them were looking at going to our new system. The point was moot as far as our old system. They all were moving on.

Senator WARNER. The Commonwealth of Virginia requested you return those machines. You did not.

Mr. LICHTENHELD. Okay.

Senator WARNER. That is the record.

Mr. LICHTENHELD. Okay.

Second, do we box customers into a service with us? No, we do not. Other vendors can provide service to our machines, and we actually make our equipment self-serviceable by our customers.

We do not need to go out and touch the equipment, for example, for our customers. We have tried to make it very much more open going forward.

Senator WARNER. So a third party could come in and be the ongoing servicer?

Mr. LICHTENHELD. Yes, and we have customers who do that.

The interoperability, that is a thing of the future probably. We are not currently working on that and that will depend on certification, and NIST, and all that good stuff.

Senator WARNER. Mr. Finney, do you want to add anything?

Mr. FINNEY. Certainly.

In terms of the three vendors sitting here today, we represent three different components of the entire electoral system. We have electronic poll book. You have a tabulation system. We happen to provide balloting to overseas, and military, and voter information tools.

The modularity of which you speak, I believe, is critical to the ongoing innovation within the elections industry, so not one vendor can own the entire electoral apparatus for one jurisdiction.

I think we do believe in letting a thousand flowers blossom by innovation and modularity, making sure that the three of us can work seamlessly together. So if Mr. Lichtenheld's system works with an electronic poll book or provides the data, so we can provide information to overseas and military voters or blind and disabled voters that we are all working together

I think that actually helps to secure and harden the overall electoral system.

Senator WARNER. The Chairman has given me discretion. I know he has got to go vote. I have to go back and vote again.

Let me just say, Mr. Chairman, I believe we have such concentration in these systems on the backend, and 90 percent concentration, and the vulnerabilities that I believe exist and still exist.

I think we need to at least think about, with this level of concentration, the ability to have potentially, at least, independent cyber security researchers having some access to give us that "Good Housekeeping Seal of Approval" at some point on some of these systems.

I am afraid if not, the vulnerability of the current, some of the self-accolades that have been given by some of the panel, may come back and bite us.

Chairman BLUNT. I am certainly willing to work with you, Senator, and see if we should look at this more closely.

I thank our witnesses for being here.

The record will be open for 1 week. I would ask you to respond quickly if you get questions in writing.

[The information referred to was submitted for the record.]

Chairman BLUNT. The committee is adjourned.

[Whereupon, at 12:24 p.m., the hearing was adjourned.]

APPENDIX MATERIAL SUBMITTED

Senate Rules and Administration Committee Hearing:
"Election Security Preparations: Federal and Vendor Perspectives"
July 11, 2018
Submitted Testimony
Commissioner Thomas Hicks, Chair, and Commissioner Christy McCormick, Vice Chair,
United States Election Assistance Commission (EAC)

Good morning, Chairman Blunt, Ranking Member Klobuchar, and members of the committee. We are pleased to appear before you today to offer testimony that supplements the written testimony the Election Assistance Commission (EAC) previously submitted for the record ahead of this committee's June 20, 2018, election security hearing.

The EAC takes very seriously its responsibility to support state and local election leaders in their efforts to conduct efficient, accessible, and secure elections. The EAC also is dedicated to providing voters the vital resources and assistance they need to register to vote and to cast their ballots, and continually equipping our partners in Congress, state and local government, private industry, advocacy organizations, other federal agencies, academia, and others in the elections industry with the information they require and rely on through our national clearinghouse.

As emphasized by one of the witnesses in the June 20 hearing, the EAC focuses solely on elections, and this focus is of great value to election administrators. Today, you will also hear from some of our federal partners who specialize in technology and cyber security. The EAC works with these and other federal entities—including the Department of Defense, the Department of Justice, and United States Postal Service, among others—to help bridge the expertise of those organizations into the context of the broad array of responsibilities facing election administrators.

The topic of today's hearing, election security, is not new to the state and local officials who run elections or the tens of thousands of election administration staff members and election workers who support and work with them, and it is not new to the EAC. The EAC has attached a diagram at the end of this testimony to demonstrate the many different components that require election administrator awareness and attention. The EAC works on each of those identified areas, including on election security, coordinating with our federal partners for additional support. It is worth noting that some of the witnesses for today's hearing have election components that fall under the statutory oversight of the EAC, particularly in the EAC's role of of implementing voluntary voting system guidelines, and federal testing and certification of the voting systems.

In this 2018 election year, providing election security tools and resources to state and local officials is one of the most important responsibilities of the EAC. Much is riding on the shoulders of local election officials. These officials, and their state colleagues, work endlessly and tirelessly—often with very modest pay compared to their government peers—to deliver upon the high expectations our country has of them. As the only federal agency focused solely on election administration, the EAC Commissioners and staff are privileged to have the opportunity to support these faithful and conscientious public servants, who are perpetually focused on ensuring that the nation has secure elections.

Election security, indeed, is an integral component of the EAC's support. In just the last 12 months, the EAC has been expeditiously distributing the newly appropriated Help America Vote Act (HAVA) funds to the states, assisting our federal partners in establishing and managing the critical infrastructure operational framework, continuing to test and certify voting systems, and highlighting and distributing important best practices in election administration as we all look ahead to the 2018 midterm election and beyond. This document briefly touches on some of those elements.

Distributing Newly Appropriated HAVA Funds

In the Consolidated Appropriations Act of 2018, Congress appropriated $380 million dollars in HAVA funds to the states and eligible territories for projects and programs to improve the administration of federal elections. In just over 3 months, the EAC has received disbursement requests for 91% of the funds from 48 of the 55 states/territories, a remarkable percentage that continues to grow daily, and 100% of the funds are available for the eligible states and territories to draw down.

The EAC issued Notice of Grant Award letters to each state less than two weeks after the bill was signed into law by President Trump. Within three weeks of the signing, Missouri, the first state to do so, had requested its funds. In the subsequent 10 weeks, the EAC conducted a webcasted public forum to explain how the funding would proceed, worked directly with the National Association of Secretaries of State (NASS) and the National Association of State Election Directors (NASED) to share information, conducted multiple webinars to further discuss how the funds may be used, consulted with members of the disability community to hear their views on use of the funds, and had frequent contact with each state in an effort to move the funds quickly.

The EAC website provides access to a set of Frequently Asked Questions regarding the funds, and this information has been updated on a near-daily basis since the law was enacted. The attached map, also on the EAC website (www.eac.gov), shows the amount of funds appropriated to each state and indicates the states that have submitted disbursement requests as of July 5, 2018. The EAC has fulfilled its promise to get the funds to the states as quickly as possible, and the EAC is proactively consulting with each of the states and territories regarding the proper use of the funds.

Several administrative issues have arisen in the funds disbursement process and the EAC's grants department is endeavoring to help the states navigate those issues so they may receive the funds in advance of the coming elections. One roadblock was the ongoing government-wide issue with System for Awards Management (SAM) accounts; the EAC's grants department is working alongside our federal partners at the Government Services Administration (GSA) to provide additional support to the EAC's SAM account holders in order to get the funds properly distributed.

The funds are being disbursed with agreement by the states to provide a short narrative describing plans for how the funds will be used, and details from these documents will be shared with the entire election community and on the EAC website, as robust information sharing is an essential component of the EAC's approach to use of these HAVA funds. It is essential that the states and territories have access to the wealth of ideas and innovative approaches contained in other states' individualized planned activities as they plan their own use of the funds. As we

continue to work closely with the state and local leaders charged with spending these funds, the EAC's staff will continue to compile the information we receive so that the election community and others will have access to particulars on how the states and territories are expending their funds to further update and secure their election systems.

Critical Infrastructure Activities

The distribution of HAVA funds is only the latest example of the EAC's work related to election security. The EAC has been serving as a central partner with the Department of Homeland Security (DHS) in ensuring the success of this national security effort well before the 2017 Critical Infrastructure designation by former Secretary Jeh Johnson. The DHS has stated that the election sector's Government Coordinating Council (GCC) was formed faster than any other similar critical infrastructure sector council to date. The EAC took an early leadership role in working toward this accomplishment, and we recognize it as an exemplary proof-point of how local, state, and federal governments can effectively work together toward the shared goal of protecting our nation's election infrastructure.

Building on that success, the EAC also convened discussions between election system vendors and the DHS for the formation of the Sector Coordinating Council (SCC). Thanks to the swift establishment of the GCC and the well-established relationships between the EAC and election equipment vendors, work on the SCC began in the summer of 2017 and its official formation meeting took place before the end of last year. Both councils were functioning before the 2018 election year and less than one year from the Critical Infrastructure designation by the DHS.

During the 2016 election cycle, the EAC was a key player in federal efforts to share vital security information with the states and educate our federal partners about ways to best serve the needs of election administrators. For example, the EAC:

- Distributed urgent security alerts and threat indicators from the DHS and the Federal Bureau of Investigation (FBI) to states and territories to help protect election systems from specific cybersecurity threats.

- Met on multiple occasions with staff from the DHS, the FBI, and the White House to discuss specific and nonspecific threats, state and local election system security and protocols, and the dynamics of the election system and its 8,000 plus jurisdictions nationwide.

- Served as the federal government's primary communication channel to provide real-time cybersecurity information to election officials around the country. This information included current data on cyber threats, tactics for protecting election systems against these threats, and the availability and value of DHS resources for protecting cyber-assets.

- Participated in and convened conference calls with federal officials, Secretaries of State and other State Chief Election Officials, state and local election administration officials, federal law enforcement, and federal agency personnel to discuss the prospect of designating elections as part of the nation's critical infrastructure. These discussions

focused on topics such as coordinating security flashes from the FBI, the implications of a critical infrastructure designation, education on the nation's election system, and the dynamics of successfully communicating information to every level of election officials responsible for running the nation's election system.

- Provided DHS with perspective, information, and data related to the election system, introductions to officials in the election community, and information that assisted the agency with shaping communications in a manner that would be useful to the states and local election officials.
- Published a white paper entitled "U.S. Election Systems as Critical Infrastructure" that provided a basic understanding of critical infrastructure for election officials.
- Contributed to multiple foundational DHS documents used to structure the Elections Systems Critical Infrastructure designation and sector.

The EAC Chair serves on the GCC Executive Committee and all EAC Commissioners were established as members of the GCC. Like many members of the GCC, the EAC is seeking security clearances through the DHS and has been assured that the department will be addressing those security requests soon.

Tactically in 2018, the EAC has focused on steps our commission could take to further serve election officials operating in this new threat environment. The EAC gathered election officials, security officials, academics, and federal government partners for an Election 2018 kick-off summit at the National Press Club in January. This event raised awareness of the security preparations election officials had underway and the resources available to the states and localities to help with this critical work. In April, the EAC held a live-streamed public forum expressly comprised of election officials to facilitate the sharing of security best practices among election colleagues

While talking about election security at forums is important, the EAC also knows the importance of training. EAC staff was intricately involved in the establishment of Harvard University's Belfer Center Table Top Exercises, which have since been conducted across the country. During the past year, EAC staff has also developed and presented its "Election Official as IT Manager" training to officials representing hundreds of election jurisdictions across the country, and we are working with the DHS to put this training online through the FedVTE platform so that many more election officials can easily access it.

The EAC also produced a video and supporting meeting materials to help local election officials explain the many levels of election security at their jurisdiction. The video was designed to be viewed at civic group meetings and election worker trainings. It can also be customized by jurisdictions, and some states are tailoring the video to their voters and processes. We plan further work in this regard. In addition, the EAC Commissioners continuously meet with state and local election officials at regional conferences across the country. These visits allow the Commissioners to apprise officials of best practices, promote resources available from the EAC

and our federal partners in agencies such as the United States Postal Service, the Federal Voting Assistance Program (FVAP) within the Department of Defense, the Department of Justice, and the DHS, and hear about and discuss current concerns and topics in election administration, such as contingency planning, accessibility, voter registration, and technology management.

Testing and Certification/Voluntary Voting System Guidelines

The EAC is authorized under the Help America Vote Act to administer federal testing and certification of voting systems. This testing standard is contained in the EAC's Voluntary Voting System Guidelines (VVSG), and vendors may choose to have EAC-accredited and monitored labs test voting systems against these guidelines for certification. The guidelines contain requirements for security, as well as other important components—such as accessibility, usability, and interoperability. In fact, while security is a guiding consideration of certification, so is accessibility for voters with disabilities and those who have limited English proficiency. These considerations are deliberated and developed in public working groups under the direction of National Institute of Science and Technology (NIST), the Director and Undersecretary of Commerce for Standards and Technology of which, Dr. Walter G. Copan, chairs the EAC's Technical Guidelines Development Committee (TGDC). This committee's membership is made up of technical and scientific experts from fields such as security, accessibility, voting machine production, and voting machine use. After development and approval by the TGDC, the voluntary guidelines are submitted to the EAC's Executive Director, provided to the EAC's two other statutory Committees, the Standards Board and the Board of Advisors, published for public comment, and presented to the EAC's Commissioners for consideration and approval.

The EAC recently convened its advisory boards to review and comment on the adoption of the newest version of the voluntary guidelines, VVSG 2.0. Both Boards recommended that the EAC adopt VVSG 2.0. The EAC, however, is currently without its minimum number of three commissioners needed for a quorum to vote on the VVSG.

While the EAC has been hard at work on the newest version of the VVSG, the EAC has not stopped its ongoing work to rigorously review, test, and certify voting machines submitted by vendors. These reviews are referred to as test campaigns, conducted by laboratories certified by the EAC. Once a system successfully completes a test campaign, the results of the campaign are transmitted to the EAC's Executive Director for certification of the voting system to the standard against which it was tested. If the EAC's Executive Director agrees that the voting system has conformed with the standard, it is certified as such and assigned a certification number.

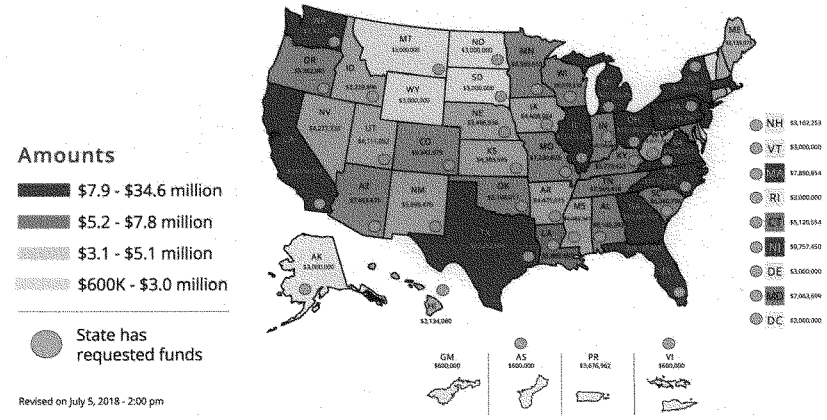
In addition to the actual certification of the voting systems, the EAC's Testing and Certification Program continually conducts quality monitoring of all EAC certified systems and audits the quality of the EAC accredited test labs. Monitoring of the voting systems occurs throughout the entire span of manufacturing and life of service, including manufacturing facility audits, field system review and testing, and field anomaly reporting from manufacturers and election officials.

Conclusion

Senators, the EAC's mission includes supporting election officials across the country with the administration of federal elections, and we endeavor to provide as much support and assistance

as possible to the state and local election officials we serve. The importance of election security and how the newly appropriated HAVA Funds will assist states with meeting these objectives are the Commission's top priority and part of our primary focus. We are honored to support the important and great work carried out by election administrators each and every day. We welcome your feedback, and we look forward to answering questions you may have.

2018 HAVA Funds




Election Officials must be experts in...
ADA
Candidates + Campaign Finance
Human Resources
Provisional Ballots
Voter Registration
Security
Military & Overseas Voting
Public Relations
Election Law
Finance
Scheduling + Logistics
Mail
Advance Voting
List Maintenance
Signature Verification
Polling Places + Real Estate
Street File Maintenance
Auditing + Recounts
Technology

Senate Rules and Administration Committee Hearing:
"Election Security Preparations: Federal and Vendor Perspectives"
July 11, 2018
Commissioner Thomas Hicks, Chair, and Commissioner Christy McCormick, Vice Chair,
United States Election Assistance Commission (EAC)

Executive Summary of Submitted Testimony

The EAC takes very seriously its responsibility to support state and local election leaders in their efforts to conduct efficient, accessible, and secure elections. The EAC also is dedicated to providing voters the vital resources and assistance they need to register to vote and to cast their ballots, and continually equipping our partners in Congress, state and local government, private industry, advocacy organizations, other federal agencies, academia, and others in the elections industry with the information they require and rely on through our national clearinghouse.

As emphasized by one of the witnesses in the June 20 hearing, the EAC focuses solely on elections, and this focus is of great value to election administrators. Today, you will also hear from some of our federal partners who specialize in technology and cyber security. The EAC works with these and other federal entities—including the Department of Defense, the Department of Justice, and United States Postal Service, among others—to help bridge the expertise of those organizations into the context of the broad array of responsibilities facing election administrators.

In this 2018 election year, providing election security tools and resources to state and local officials is one of the most important responsibilities of the EAC. Much is riding on the shoulders of local election officials. These officials, and their state colleagues, work endlessly and tirelessly—often with very modest pay compared to their government peers—to deliver upon the high expectations our country has of them. As the only federal agency focused solely on election administration, the EAC Commissioners and staff are privileged to have the opportunity to support these faithful and conscientious public servants, who are perpetually focused on ensuring that the nation has secure elections.

Election security, indeed, is an integral component of the EAC's support. In just the last 12 months, the EAC has been expeditiously distributing the newly appropriated Help America Vote Act (HAVA) funds to the states, assisting our federal partners in establishing and managing the critical infrastructure operational framework, continuing to test and certify voting systems, and highlighting and distributing important best practices in election administration as we all look ahead to the 2018 midterm election and beyond. Testimony today will highlight some of those activities.

Thomas Hicks
Chair
U.S. Election Assistance Commission

Thomas Hicks was nominated by President Barack H. Obama and confirmed by unanimous consent of the United States Senate on December 16, 2014 to serve on the U.S. Election Assistance Commission (EAC). Thomas Hicks became the Chairman of the EAC in February 2018, a position he will hold for one year. Commissioner Hicks previously served as Chairman of the EAC from February 2016 until February 2017.

During his time with EAC, Commissioner Thomas Hicks has prioritized technology improvements in the nation's election systems and better poll access. Hicks has worked to ensure that election technology purchased using HAVA funds is running to the best possible standards and that all voters – without regard to ability, language, or location – have the same opportunity to cast their ballot. Hicks has also prioritized initiatives such as online voter registration, updating the voluntary voting system guidelines, and improving efforts to recruit more poll workers to serve on Election Day.

Prior to his appointment with the EAC, Commissioner Hicks served as a Senior Elections Counsel and Minority Elections Counsel on the U.S. House of Representatives Committee on House Administration. Prior to joining the U.S. House of Representatives, Hicks served as a Senior Lobbyist and Policy Analyst for Common Cause, a nonpartisan, nonprofit organization that empowers citizens to make their voices heard in the political process and to hold their elected leaders accountable to the public interest. Hicks served in the Clinton Administration as a Special Assistant and Legislative Assistant in the Office of Congressional Relations for the Office of Personnel Management. He served as agency liaison to the United State Congress and the President's Administration on matters regarding federal personnel policies and regulations.

Christy McCormick
Vice Chair
U.S. Election Assistance Commission

Christy McCormick was nominated by President Barack H. Obama and confirmed by unanimous consent of the United States Senate on December 16, 2014 to serve on the U.S. Election Assistance Commission (EAC). Commissioner McCormick became Acting Vice Chair of the EAC in February 2018, a position she will hold for one year. Commissioner McCormick served as the Chairwoman of the EAC from February 2015 until February 2016. McCormick was the first chair of the agency following a nearly five-year period where there were not enough Commissioners to hold public meetings.

During her time at the Election Assistance Commission, Commissioner McCormick has worked to ensure the accuracy and integrity of American elections while increasing voter participation. As a former overseas voter, she has been a powerful advocate for military and overseas voters, working to ensure they are able to participate in the voting process without delay or difficulty.

Prior to her appointment with EAC, Commissioner McCormick served as a Senior Trial Attorney in the Voting Section of the Civil Rights Division at the Department of Justice. McCormick was detailed by the Deputy Attorney General to be Senior Attorney Advisor and Acting Deputy Rule of Law Coordinator in the Office of the Rule of Law Coordinator at the U.S. Embassy in Baghdad, Iraq from 2009 to 2010, where she worked on the Iraq national elections and on rule of law matters. McCormick was a U.S. elections expert in Iraq observing and monitoring the 2010 Iraq National elections, providing assistance and advice to the Independent High Electoral Commission and witnessing an extensive 12-day election recount. She was a rule of law liaison to the Kurdish Regional Government and a liaison to rule of law advisors at the Provincial Reconstruction Teams.

Prior to joining the Department of Justice, McCormick served as a Judicial Clerk to the Honorable Elizabeth A. McClanahan in the Court of Appeals of Virginia. McCormick was an Assistant Attorney General and Assistant to the Solicitor General in the Office of the Attorney General of Virginia. She was a Judicial Law Clerk in Virginia's Seventh Judicial Circuit Court.

Testimony of

Charles H. Romine, Ph.D.

Director
Information Technology Laboratory
National Institute of Standards and Technology
United States Department of Commerce

Before the
United States Senate
Committee on Rules and Administration

"*Election Security Preparations: Federal and Vendor Perspectives*"

July 11, 2018

Introduction

Chairman Blunt, Ranking Member Klobuchar, and members of the Committee, I am Charles Romine, the Director of the Information Technology Laboratory (ITL) at the Department of Commerce's National Institute of Standards and Technology (NIST). Thank you for the opportunity to appear before you today to discuss our role in what NIST is doing in election security.

The Role of NIST in Cybersecurity

Home to five Nobel Prizes, with programs focused on national priorities such as advanced manufacturing, the digital economy, precision metrology, quantum science, and biosciences, NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

In the area of cybersecurity, NIST has worked with federal agencies, industry, and academia since 1972, when it helped develop and published the data encryption standard, which enabled efficiencies like electronic banking that we all enjoy today. NIST's role, to research, develop, and deploy information security standards and technology to protect the Federal Government's information systems against threats to the confidentiality, integrity, and availability of information and services, was strengthened through the Computer Security Act of 1987 (Public Law 100-235), broadened through the Federal Information Security Management Act of 2002 (FISMA) (Public Law 107-347)[1] and reaffirmed in the Federal Information Security Modernization Act of 2014 (FISMA 2014) (Public Law 113-283). In addition, the Cybersecurity Enhancement Act of 2014 (Public Law 113-274) authorizes NIST to facilitate and support the development of voluntary, industry-led cybersecurity standards and best practices for critical infrastructure.

NIST also coordinates with numerous other federal agencies, as well as its sister bureaus within the Department of Commerce. For example, as the executive branch agency principally responsible for advising the President on telecommunications and information policies, the Commerce Department's National Telecommunications and Information Administration, collaborates with NIST to ensure that the equities of innovation, economic growth, and an open Internet are factored into cybersecurity policy decisions within both domestic and international fora.

NIST develops guidelines in an open, transparent, and collaborative manner that enlists broad expertise from around the world. These resources are used by federal agencies as well as businesses of all sizes, educational institutions, and state, local, and tribal governments, because NIST's standards and guidelines are effective, state-of-art and widely accepted. NIST disseminates its resources through a variety of means that encourage the broad sharing of tools, security reference data, information security standards, guidelines, and practices, along with outreach to stakeholders, participation in government and industry events, and online mechanisms.

[1] FISMA was enacted as Title III of the E-Government Act of 2002 (Public Law 107-347).

NIST Cybersecurity Framework

I would like to highlight some changes to a document that the Committee may be familiar with: the Framework for Improving Critical Infrastructure Cybersecurity (the "Framework"), which many organizations—including many state governments—use to manage their cybersecurity risk. Beginning in 2013, NIST created, promoted, and continues to enhance the Framework in collaboration with industry, academia, and other government agencies. The Framework consists of voluntary standards, guidelines, and practices to promote the protection of critical infrastructure. The Framework's voluntary, risk-based, flexible, repeatable, and cost-effective approach helps users manage their cybersecurity risk. The Framework was originally designed for owners and operators of critical infrastructure, but organizations of all sizes and from many economic sectors now use the Framework to manage their cybersecurity risks, including risks to their supply chains. While use is both voluntary and widespread in the private sector, the Executive Order, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," formally requires agencies to use the Framework to manage their cybersecurity risk – something many agencies did prior to its issuance.

In response to stakeholder requests, NIST began the public engagement process to update the Framework. This process included NIST examining lessons learned from use of the Framework, collecting written comments, hosting multiple workshops, incorporating comments and feedback, and issuing multiple drafts before publishing the final updated version 1.1 in April 2018. The Framework continues to be a living document which draws strength from active and voluntary private-sector contributors.

The Role of NIST in Voting Systems

NIST's role in helping secure our Nation's voting systems draws on our expertise in providing measurements, working with standards development organizations and stakeholder communities, and the development of testing infrastructures necessary to support standards implementation.

Improving voting systems requires an interdisciplinary, collaborative approach. The systems must be accurate and reliable, yet cost-effective. They must be secure and usable. And, they must be accessible to all voters, allowing them to vote independently and privately. Their design and the underlying standards must take into consideration the diversity of voting processes and ballots across the states. None of these can be considered in a vacuum. NIST expertise in testing, information security, trusted networks, software quality, and usability and accessibility provide the technical foundation for our voting systems work. Additionally, our experience working in multi-stakeholder processes is critical to the success of NIST's voting program.

For more than a decade, as directed by both the Help America Vote Act of 2002[2] (HAVA) and the Military and Overseas Voter Empowerment Act[3] (MOVE), the NIST Voting Program has partnered with the Election Assistance Commission (EAC) to develop the science, tools, and standards necessary to improve the accuracy, reliability, usability, accessibility, and security of voting equipment used in federal elections for both domestic and overseas voters.

---

[2] Public Law 107-252, (Oct. 29, 2002), codified in relevant part at 52 U.S.C. 20901 *et seq.*

[3] Public Law 111-84, div. A, title V, (Oct. 28, 2009), codified in relevant part at 52 U.S.C. § 20311.

Under HAVA, NIST is tasked with providing technical support to the Technical Guidelines Development Committee, Federal Advisory Committee to the EAC to which the Director of NIST serves as Chair. This support includes areas such as the security of computers, computer networks, and computer data storage used in voting systems, methods to detect and prevent fraud, protection of voter privacy, the role of human factors in the design and application of voting systems, and remote access voting, including voting through the Internet. This technical support includes intramural research and development in areas to support the development of a set of Voluntary Voting System Guidelines (VVSG or Guidelines), which upon recommendation by the Technical Guidelines Development Committee are forwarded to the EAC for further consideration prior to adoption via a quorum of EAC Commissioners. The Guidelines are used by accredited testing laboratories as part of both state and national certification processes; by state and local election officials who are evaluating voting systems for potential use in their jurisdictions; and by manufacturers who need to ensure that their products fulfill the requirements, so they can be certified.

The Guidelines address many aspects of voting systems including determining system readiness, ballot preparation and election definition, voting and ballot counting operations, safeguards against system failure and protections against tampering, ensuring the integrity of voted ballots, protecting data during transmission, and auditing. Additionally, the Voluntary Voting System Guidelines tackles physical and systems-level security.

NIST Activities Related to Election Security

Voluntary Voting System Guidelines

The Guidelines is a set of specifications and requirements against which voting systems can be tested to determine if the systems meet required standards. On December 13, 2005, the EAC unanimously adopted the 2005 Guidelines, which significantly increased security requirements for voting systems and expanded access, including opportunities for individuals with disabilities to vote privately and independently. Version 1.1 of the Guidelines was unanimously approved by the Election Assistance Commissioners on March 31, 2015. Version 1.1 made the Guidelines more testable and improved portions of the guidelines without requiring massive programmatic changes.

Almost immediately following the adoption of Voluntary Voting System Guidelines 1.1, NIST, in consultation with the EAC, established a set of a public working groups to gather input from a wide variety of stakeholders on the development of the next iteration of the Guidelines, entitled Voluntary Voting System Guidelines 2.0. This approach was consistent with NIST efforts in cloud and smart grid, where NIST convened groups of stakeholders to gather input, and served to address feedback from the Presidential Commission on Election Administration,[4] the EAC Standards Board, and the National Association of State Election Directors,[5] as well other subject matter experts across the Nation. There are currently 963 members across seven working groups, three of which are aimed at election process (pre-election, election and post-election), three groups focused on the technical underpinnings of the Guidelines (cybersecurity, usability and accessibility, and interoperability), and one that will address issues related to testing.

[4] https://www.supportthevoter.gov/
[5] https://www.nased.org/

Election Security

The cybersecurity working group has grown to 162 members, and engages in discussions regarding the security of U.S. elections. From the early 1900s, election administrators were primarily concerned with breaches of physical security, natural disasters, accidental errors, and events affecting public trust.

As voting systems have evolved, so have their security concerns. Guidelines 2.0 includes support for advanced auditing methods (such as risk-limiting audits) as well as enhanced authentication requirements. It mandates two-factor authentication for certain critical voting operations, including accessing administrative accounts, updating voting system software, performing aggregation of tabulation of ballots, and enabling networking functions. Voting systems often use commercial off-the-shelf hardware and software. The system integrity section in Guidelines 2.0 ensures that security protections developed by industry over the past decade are built into the voting system.

Other security issues to be resolved, beyond those mentioned in the Guidelines, include the need for regular and timely software update and security patches. Networked communication is another important security issue currently under discussion. Many election jurisdictions rely on public telecommunications networks for certain election functions, such as reporting results to state agencies and media outlets the night of an election. These connections, however brief, are a significant expansion of threat surface and their security requires further study.

In January 2017, the Secretary of Homeland Security designated the Nation's election infrastructure as critical infrastructure, making it a subsector of the Government Facilities Sector. NIST participates as an ex officio member of the Election Infrastructure Subsector Government Coordinating Council, alongside our federal, state, and local partners. In support of this effort, NIST is providing technical leadership in the creation of an Election Profile of the Cybersecurity Framework. This profile is another tool NIST is developing to help election officials identify and prioritize opportunities to improve their cybersecurity posture.

Testing

NIST is responsible, under HAVA, for conducting evaluations of independent, non-federal laboratories and submitting to the EAC a list of the laboratories that NIST proposes to be accredited to carry out testing, certification, decertification, and recertification of voting systems.

NIST developed "test assertions" for critical security, usability, accessibility and functionality requirements under Voluntary Voting System Guidelines 1.0 and 1.1. It is anticipated that accredited voting systems laboratories will use these NIST-developed test assertions to achieve uniformity in testing among laboratories.

Conclusion

NIST is addressing election security by strengthening the Voluntary Voting System Guidelines for voting systems, such as vote capture and tabulation, and by working with our government partners, including the EAC, to provide guidance to state and local election officials on how to secure their election systems including voter registration and election reporting systems.

Thank you for the opportunity to testify on NIST's work regarding election security. I will be pleased to answer any questions you may have.

Statement for the Record

Matt Masterson
Senior Cybersecurity Advisor
National Protection and Programs Directorate
U.S. Department of Homeland Security

FOR A HEARING ON

"Election Security Preparations: Federal and Vendor Perspectives"

BEFORE THE
UNITED STATES SENATE
COMMITTEE ON RULES AND ADMINISTRATION

Wednesday, July 11, 2018

Washington, DC

Chairman Blunt, Ranking Member Klobuchar, and members of the Committee, thank you for today's opportunity to testify regarding the U.S. Department of Homeland Security's (DHS) ongoing efforts to assist with reducing and mitigating risks to our election infrastructure. DHS is eager to share with you the progress we have made to establish trust-based partnerships with our Nation's election officials who administer our democratic election processes.

Safeguarding and securing cyberspace is a core homeland security mission. DHS is responsible for protecting civilian Federal Government networks and collaborating with other Federal agencies, as well as state, local, tribal, and territorial governments, and the private sector to defend against cyber threats. We endeavor to enhance cyber threat information-sharing across the globe to stop cyber incidents before they start and help businesses and government agencies to protect their cyber systems and quickly recover should such an attack occur. By bringing together all levels of government, the private sector, international partners, and the public, we are taking action to protect against cybersecurity risks, improve our whole-of-government incident response capabilities, enhance information sharing of best practices and cyber threats, and to strengthen resilience.

Recognizing that the 2018 U.S. mid-term elections are a potential target for malicious cyber activity, DHS is committed to robust engagement with state and local election officials, as well as private sector entities, to assist them with defining their risk, and providing them with information and capabilities that enable them to better defend their infrastructure.

Given the foundational role that elections play in a free and democratic society, in January 2017 the Secretary of Homeland Security designated election infrastructure as a critical infrastructure subsector. Under our system of laws, federal elections are administered by state and local election officials in thousands of jurisdictions across the country. These officials manage election infrastructure and ensure its security and resilience on a day-to-day basis.

As such, DHS and our federal partners have formalized the prioritization of ***voluntary*** cybersecurity assistance for election infrastructure similar to that which is provided to a range of other critical infrastructure entities, such as financial institutions and electric utilities.

Since 2016, DHS's National Protection and Programs Directorate (NPPD) has convened Federal Government and election officials regularly to share cybersecurity risk information and to determine an effective means of assistance. The Election Infrastructure Subsector (EIS) Government Coordinating Council (GCC) has worked to establish goals and objectives, including plans for EIS engagement and the establishment of a sector-specific plan (SSP). GCC representatives include DHS, the Election Assistance Commission (EAC), and 24 state and local election officials. Participation in the council is entirely voluntary and does not change the fundamental role of state and local jurisdictions in overseeing elections.

The Department and the EAC worked with election industry representatives to launch an industry-led Sector Coordinating Council (SCC), a self-organized, self-run, and self-governed council with leadership designated by the sector membership. The SCC serves as industry's principal entity for coordinating with the government on critical infrastructure security activities and issues related to sector-specific strategies, and policies. This collaboration is conducted

under DHS's authority to provide a forum in which government and private sector entities can jointly engage in a broad spectrum of activities to coordinate critical infrastructure security and resilience efforts which is used in each of the critical infrastructure sectors established under Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience*. The process is a well-tested mechanism across critical infrastructure sectors for sharing threat information among the Federal Government and critical infrastructure partners, advancing risk management efforts, and prioritizing services available to sector partners in a trusted environment.

NPPD also engages directly with election officials—coordinating requests for assistance, risk mitigation, information sharing, and incident coordination, resources, and services. In order to ensure a coordinated approach from the federal government, NPPD has convened stakeholders from across the Federal Government through an Election Task Force. The task force serves to provide actionable information and offer assistance to assist election officials with strengthening their election infrastructure by reducing and mitigating cyber risk, and increasing resilience of their processes.

Within the context of today's hearing, I will address the unclassified assessment of malicious cyber operations directed against U.S. election infrastructure and our efforts to help enhance the security of elections that are administered by jurisdictions around the country.

Enhancing Security for Future Elections

DHS regularly coordinates with the intelligence community and law enforcement partners on potential threats to the Homeland. Among non-federal partners, DHS has been engaging state and local officials, as well as relevant private sector entities, to assess the scale and scope of malicious cyber activity potentially targeting the U.S. election infrastructure. Election infrastructure includes the information and communications technology, capabilities, physical assets, and technologies that enable the registration and validation of voters; the casting, transmission, tabulation, and reporting of votes; and the certification, auditing, and verification of elections.

DHS is committed to ensuring a coordinated response from DHS and its federal partners to plan for, prepare for, and mitigate risk to election infrastructure. We understand that working with election infrastructure stakeholders is essential to ensuring a more secure election. DHS and our stakeholders are increasing awareness of potential vulnerabilities and providing capabilities to enhance the security of U.S. election infrastructure as well as that of our democratic allies.

Election officials across the country have a long-standing history of working both individually and collectively to reduce risks and ensure the integrity of their elections. In partnering with these officials through both new and ongoing engagements, DHS is working to provide value-added—yet voluntary—services to support their efforts to secure elections.

Improving Coordination with State, local Tribal, Territorial (SLTT) and Private Sector partners. Increasingly, the nation's election infrastructure leverages information technology (IT) for efficiency and convenience, but also exposes systems to cybersecurity risks,

just like in any other enterprise environment. Just like with other sectors, NPPD helps stakeholders in federal departments and agencies, SLTT governments, and the private sector to manage these cybersecurity risks. Consistent with our long-standing partnerships with state and local governments, we have been working with election officials to share information about cybersecurity risks, and to provide voluntary resources and technical assistance.

The National Cybersecurity and Communications Integration Center (NCCIC) works with the MS-ISAC to provide threat and vulnerability information to state and local officials. For nearly a decade, DHS has funded the Multi-State Information Sharing and Analysis Center (MS-ISAC), which has since created the EI-ISAC, to enable its members to share cybersecurity information and collaborate with each other. The EI-ISAC's membership includes almost 1,000 SLTT election-specific entities. Through the MS-ISAC, it has representatives co-located with the NCCIC to enable regular collaboration and access to information and services for state chief information officers.

Providing Technical Assistance and Sharing Information. NPPD actively promotes a range of services including:

Cyber hygiene service for Internet-facing systems: Through this automated, remote scan, NPPD may provide a report identifying vulnerabilities and mitigation recommendations to improve the cybersecurity of systems connected to the Internet, such as online voter registration systems, election night reporting systems, and other Internet-connected election management systems.

Risk and vulnerability assessments: We have prioritized state and local election systems upon request, and increased the availability of risk and vulnerability assessments (RVAs). These in-depth, on-site evaluations include a system-wide understanding of vulnerabilities, focused on both internal and external systems. We provide a full report of vulnerabilities and recommended mitigations following the testing.

Incident response assistance: We encourage election officials to report suspected malicious cyber activity to the NCCIC. Upon request, the NCCIC can provide assistance in identifying and remediating a cyber incident. Information reported to the NCCIC is also critical to the federal government's ability to broadly assess malicious attempts to infiltrate election systems. This technical information will also be shared with other state officials so they have the ability to defend their own systems from similar malicious activity.

Knowing what to do when a security incident happens—whether physical or cyber—before it happens, is critical. NPPD supports election officials with incident response planning including participating in exercises and reviewing incident response playbooks. Crisis communications are a core component of these efforts, ensuring officials are able to communicate transparently and authoritatively to their constituents when an incident unfolds. In some cases, we do this directly with state and local jurisdictions. In others, we partner with outside organizations. We recognize that securing our nation's systems is a shared responsibility, and we are leveraging partnerships to advance that mission.

Information sharing: NPPD maintains numerous platforms and services to share relevant information on cyber incidents. State election officials may also receive information directly from the NCCIC. The NCCIC also works with the EI-ISAC, which allows election officials to connect with the EI-ISAC or their State Chief Information Officer to rapidly receive information they can use to protect their systems. Best practices, cyber threat information, and technical indicators, some of which had been previously classified, have been shared with election officials in thousands of state and local jurisdictions. In all cases, the information sharing and/or use of such cybersecurity risk indicators, or information related to cybersecurity risks and incidents complies with applicable lawful restrictions on its collection and use and with DHS policies protective of privacy and civil liberties.

Classified information sharing: To most effectively share information with all of our partners—not just those with security clearances—we work with the intelligence community to rapidly declassify relevant intelligence or provide tearlines. While DHS prioritizes declassifying information to the extent possible, we also provide classified information to cleared stakeholders, as appropriate. DHS has been working with state chief election officials and additional election staff in each state to provide them with security clearances. By working with ODNI and the Federal Bureau of Investigation (FBI), in February 2018 election officials from each state received one-day read-ins for a classified threat briefing while they were in Washington, DC. This briefing demonstrated our commitment to ensuring election officials have the information they need to understand the threats they face.

Field-based cybersecurity advisors and protective security advisors: NPPD has more than 130 cybersecurity and protective security personnel available to provide actionable information and connect election officials to a range of tools and resources to improve the cybersecurity preparedness of election systems; and to secure the physical site security of voting machine storage and polling places. These advisors are also available to assist with planning and incident management for both cyber and physical incidents.

Physical and protective security tools, training, and resources: NPPD provides guidance and tools to improve the security of polling sites and other physical election infrastructure. This guidance can be found at www.dhs.gov/hometown-security. This guidance helps to train administrative and volunteer staff on identifying and reporting suspicious activities, active shooter scenarios, and what to do if they suspect an improvised explosive device.

Election Security Efforts Moving Forward

DHS has made tremendous strides and is committed to working collaboratively with those on the front lines of administering our elections to secure election infrastructure from risks. The establishment of government and sector coordinating councils will build the foundations for this enduring partnership not only in 2018, but for future elections as well. We will remain transparent as well as agile in combating and securing our physical and cyber infrastructure. However, we recognize that there are significant technology needs across SLTT governments, and State and local election systems, in particular. It will take significant and continual investment to ensure that election systems across the nation are upgraded and secure, with

vulnerable systems retired. These efforts require a whole of government approach. The President and this Administration are committed to addressing these risks.

There is a fundamental link between public trust in our election infrastructure and the confidence the American public places in basic democratic functions. Ensuring the security of our electoral process is a vital national interest and one of our highest priorities. Our voting infrastructure is diverse, subject to local control, and has many checks and balances. As the threat environment evolves, we will continue to work with federal agencies, state and local partners, and private sector entities to enhance our understanding of the threat; and to make essential physical and cybersecurity tools and resources available to the public and private sectors to increase security and resiliency.

Thank you for the opportunity to appear before the Committee today, and I look forward to your questions.

SCOTT LEIENDECKER
U.S. Senate Committee on Rules and Administration
Hearing on Election Security Preparations: Vendor Perspective
Wednesday, July 11, 2018

Chairman Blunt, Ranking Member Klobuchar, and members of the Committee, thank you for today's opportunity to be with you today. I'm grateful for your willingness to engage and take into consideration the vendor perspective. I'm truly honored to be part of this discussion and hope that my testimony will be constructive and helpful.

It seems concerns about election security over the past 14 months has hit an all-time high. I cannot talk about what outsiders or so called hackers are trying to do to disrupt our most sacred process. What I can speak with you about today are the initiatives companies like mine are doing to prevent, detect and defend against any such attacks so we can effectively preserve the security and integrity of American elections.

The Congress and Presidents in both parties have recognized the need more efficient and accessible elections. President Bush signed the bipartisan Help American Vote Act in 2002 to help improve voter access and voting systems. In his 2013 State of the Union Address, President Obama highlighted a 102-year-old North Miami woman who had to wait six hours to vote. Unacceptable.

I served at the St. Louis Board of Elections for six years. At that time, I saw how emerging technologies could help make the voting process easier for everyone. Unfortunately, few products were available to election officials like me and the products that were available were seemingly outmoded as soon as we brought them online.

When I founded my business, I wanted to leverage technology to make our election process better for voters, election officials and taxpayers. To start, I wanted to create a solution to the outmoded, outdated paper poll books that have often been responsible for long lines at the polls, especially during peak voting hours.

The technology we use in our signature product, the Poll Pad, is an iPad-based system that eliminates paper poll books and the A through K lines, allowing voters to check in to their polling place in just a few short steps, reducing wait times and keeping voting lines moving more swiftly. After an election, our technology allows election officials to easily catalog the information from election day instead of the old way of transferring information from paper books to electronic systems. These efficiencies are better for election workers and taxpayers.

Like the Department of Defense, the Department of Justice and others in the federal government that use iPads in special use cases, we selected the iPad platform because of the security baked into these devices within the IOS

operating system. We harden the iPads by following strict guidelines to help set them up in a secure manner. We use security features like two-factor authentication and a secure hosting environment using encryption algorithms approved by the National Institute of Standards and Technology. This prevents sensitive data from not only being exposed where it shouldn't but also prevents it being manipulated by third parties. In short, we rely on security experts and the latest technologies to create a strong security infrastructure for our products.

In order to continue innovating and providing stronger security initiatives, we hope the federal government will consider us a partner.

We hope today's hearing is just the beginning of a new conversation this committee and the federal government will have with election vendors. Together with local election officials we are on the front lines on election day and throughout the elections process. We want to offer this committee and others in the federal government our assistance to help shape public policy to ensure the integrity of our most sacred process.

###

Statement for the Record

Peter Lichtenheld

Vice President of Operations

Hart InterCivic, Inc.

For a hearing on

Election Security Preparations: Federal and Vendor Perspectives

Before the

United States Senate

Committee on Rules and Administration

July 11, 2018

Executive Summary: Voting system companies are a critical part of the Election Security solution, in partnership with federal, state and local election officials and agencies, to help protect the integrity of the vote in America. At least as important as voting system technology are the people, processes and procedures in use by election officials to ensure the sanctity of the vote. We, the voting system providers, and Hart specifically, are fully engaged in the conversation about and renewed focus on elections security, for example with the Department of Homeland Security through the Sector Coordinating Council, with the Center for Internet Security and with our customers.

Hart InterCivic is based in Austin, Texas where we have been located since our inception over 100 years ago. Hart began as a paper ballot printer and we've evolved to become one of the top three voting system providers in the country, with customers across 18 states. Hart's business is focused exclusively on voting systems.

While Hart maintains strong working relationships with many federal and state officials and groups, our primary customers are local, usually county, election administrators, auditors and clerks charged with overseeing local government in general and elections in particular.

We agree with the DHS and EAC approach of defend, detect and recover. We also encourage, and we employ, a defense-in-depth approach. All Hart voting systems go through thorough, independent testing to achieve required federal and state certifications before they are used. Hart systems utilize the very latest in software and hardware security technology and support rigorous post-election audits.

Election experts refer to the importance of cultivating secure election management through a combination of "people, processes, procedures and technology." We are fully supportive of America's election officials and poll workers and we salute their dedication and hard work as we assist them in developing and implementing best practices around people, processes, procedures and technology.

Hart InterCivic is dedicated to election security through our involvement in the current dialog about election security as critical infrastructure, through the technologies that we offer, through sharing best practices with our customers and through our firm belief in the sanctity of the vote and the importance that the American public has confidence that every vote counts.

Bio: Peter Lichtenheld, CERA

Vice President of Operations

Hart InterCivic, Inc.

As Vice President of Operations, Mr. Lichtenheld is the Company's point person on all industry-wide discussions and activities surrounding Election Security. This includes being Hart's primary representative on the Department of Homeland Security's election infrastructure industry Sector Coordinating Council.

In addition, Mr. Lichtenheld oversees and coordinates timely and accurate delivery of numerous customer-critical services. His management of Product Management, Certification, Ballot Production Services, Technical Services, Professional Services and the Customer Support Center is key to customers receiving voting system components, services and on-going support.

Prior to joining Hart in 2001, Mr. Lichtenheld worked as an educator, specializing in training programs from elementary level to adult learning programs for doctoral level students. This experience was valuable to his development of Hart's comprehensive voting system training programs that benefit election officials, poll workers, and technicians in thousands of jurisdictions across the country. Pete has worked as team leader in all aspects of Hart's elections business. He was instrumental in organizing Hart's Customer Support Center and leads company initiatives focusing on the customer experience.

Mr. Lichtenheld received a Master of Arts in Instructional Technology from the University of Texas at Austin and a Bachelor of Arts degree in Religious Studies and Philosophy from Beloit College in Wisconsin. He is a State of Texas certified teacher and a graduate of the Certified Elections/Registration Administrator/Vendor program with The Election Center, where he continues ongoing education.

Written Testimony: Chairman Blunt, Ranking Member Klobuchar and members of the Committee, thank you for the invitation and for the opportunity to speak with you about the critically important topic of Election Security. My name is Peter Lichtenheld and I serve as the Vice President of Operations at Hart InterCivic.

Hart InterCivic believes that voting system companies are a critical part of the Election Security solution, in partnership with federal, state and local election officials and agencies, to help protect the integrity of the vote in America. At least as important as voting system technology are the people, processes and procedures in use by election officials to ensure the sanctity of the vote. The voting system providers, and Hart specifically, are fully engaged in the conversation about and renewed focus on elections security, for example with the Department of Homeland Security through the Sector Coordinating Council, with the Center for Internet Security and with our customers.

Hart InterCivic is based in Austin, Texas where we have been located since our inception over 100 years ago. Hart began as a paper ballot printer and we've evolved to become one of the top three voting system providers in the country, with customers across 18 states. Hart's business is focused exclusively on voting systems, including software and devices used to define elections, create ballots, capture votes, tabulate votes, report and audit the results. We are not involved in voter registration solutions nor any other aspect of elections or government administration. Hart's voting systems are designed, engineered and manufactured in the USA in the State of Texas.

While Hart maintains strong working relationships with many federal and state officials and groups, our primary customers are local, usually county, election administrators, auditors and clerks charged with overseeing local government in general and elections in particular. Hart is not a "one size fits all" voting system provider. Most local election officials, within the bounds of state law, have significant flexibility and latitude in determining how elections will run in their jurisdiction. Functional needs and preferences vary from state to state and even county to county within a state. Election officials choose the voting style and we support them and provide the technology they choose. This may include by-mail voting or all the various methods of in-person voting from hand-marked paper ballots to hybrid systems which combine electronic voter interfaces with a hard-copy paper trail. We actively seek feedback from customers and prospective customers, incorporate their input, and evolve our solutions as needed. We do this to ensure we deliver the best possible technology solutions to election officials and to keep up with the evolving needs and requirements of those officials.

We agree with the DHS and EAC approach of defend, detect and recover. Here's how we support that approach:

- Hart InterCivic engages fully with the DHS and with the Center for Internet Security. We are glad to be part of the Sector Coordinating Council, working with other election providers and with the Government Coordinating Council to defend the critical infrastructure of our nation's elections.
- Before they are used in any election, all elements of Hart voting systems are submitted for thorough security and performance testing by an independent, accredited and approved voting system testing laboratory as part of a federal certification process overseen by the U.S. Election

Assistance Commission (or EAC). Certified voting systems adhere to standards designed to ensure that systems accurately record votes the way they are cast. Security standards include protections against tampering or manipulation and cover requirements for physical security of the equipment and ballots, features that prevent connection to the internet or a network, auditing capabilities and more.

- In addition to federal-level testing by the U.S. EAC, most states require separate and additional security and performance testing and certification of voting systems before they may be sold in those states. Hart systems have been certified in all 18 states where we do business, and we are currently in the certification process in several more.
- We have a strong approach to security evident in the design of all elements of our voting system technologies. Security features of Hart voting systems include:
    - Hart voting systems are NOT connected to the internet. Hart voting systems are in NO way connected to: Internet, Intranet or in-office networks, voter rolls/registration, voter personal data, campaign/donor information, party/campaign volunteer information or schedules, Voter communications regarding times/locations for early or Election Day voting, or Email systems.
    - Cast vote record data is digitally signed using NIST-compliant FIPS 140-2 cryptographic modules.
    - Multiple redundant data backups ensure that any malicious data manipulation would be detected by comparing data sets during an audit (e.g., compare paper ballots to electronic cast vote records).
    - Application whitelisting prevents unauthorized computer programs or code from being executed on voting devices and on computers that run Hart's election software. (Whitelisting is a more stringent anti-virus approach that looks at what IS allowed to run on the system vs. traditional anti-virus applications that looks at what is NOT allowed to run on the system.)
    - Hart's voting system software cannot be remotely accessed by Hart or anyone else, including remote access for troubleshooting (no remote desktop).
    - Systems running Hart's voting system software operate in "kiosk" mode, which means the user can only access those functions required by the software. This prevents user access to the operating system and prevents installation of any unauthorized programs or files onto the system. The system is "locked down" to prevent intentional or accidental misuse by the operator.
    - On Hart voting devices, external cards, drives, cables or other devices cannot be inserted by voters.
    - Multiple keyed locks restrict access to voting devices and memory devices.
    - Devices are designed for use with tamper-evident seals.
    - Devices use non-standard electrical wiring in strategic areas.
    - Two-factor authentication is used to secure access to critical election management functions.
    - Every application and device thoroughly logs all user authentication, data entry, user interaction, and system events. Election managers can print or export plain language audit logs from each application, using easy-to-use report filtering to access the precise information to be audited.

- Hart supports the most rigorous post-election audits. Audit features allow election officials to maintain and access a detailed electronic record of all activities that occur related to the system, as well as the ability to review cast vote data to verify the results and detect any errors. Auditing is not only a big part of election security and verification of results but is also instrumental in the ability to detect attempted data manipulation. We believe that every state should have mandatory and consistent audit requirements and that audits should be conducted for every election. Audits help to provide voter confidence in the franchise.

While voting system technology is an important aspect of security, true election security also requires thoroughly trained election officials and staff upholding government-defined processes by implementing well-honed election management procedures. Election experts refer to the importance of cultivating secure election management through a combination of "people, processes, procedures and technology." This is all a part of the defense-in-depth approach to security, which we fully embrace. We are supportive of America's election officials and poll workers and we salute their dedication and hard work. We regularly provide Best Practices newsletters, webinars, articles and individualized one-on-one consultations for our customers and for all election officials in America. Some of our best practices around People, Processes and Procedures include:

- We recognize that individual jurisdictions' election managers are responsible for the "people" aspect of election security. We encourage and train election leaders to ensure staff members and temporary workers are carefully selected and properly vetted with reference and background checks. Election personnel require training, including cross-training, in the procedures and technology used to ensure accurate vote capture and tabulation. Team members should be assigned unique usernames, passwords and permissions to access only the appropriate functions within the voting system. Additionally, two people should be present for certain types of functions. To assist our customers in keeping their staff members' knowledge of our systems fresh and relevant, we offer our customers free training for new election managers who have come on board after the initial system implementation and training events.
- Government bodies (typically states) establish the "process" aspect of election security in the form of election laws, code, rules and advisories. Local jurisdictions within each state must stay informed of these processes and adhere to them. We help our customers to make certain that they are compliant with state rules, laws and advisories where it is appropriate that we do so.
- Responsibility for the "procedures" aspect of election security resides with jurisdictions' election managers. Local procedures document how to apply state election law, rules and advisories based on the jurisdiction's election technology. Procedures include the frequency and written steps for testing the voting system's logic and accuracy for every election before any ballots go out to the public, chain-of-custody protocols for voting equipment, rules for who can access voting system software, reconciliation of election results with the voter count for every election, post-election audit steps and more. Election managers love checklists, and we think of Procedures as those checklists. We assist with system-related procedures by providing effective training and comprehensive documentation, including checklists, to our customers.

Hart remains actively engaged in the national conversation on election security. We are connected with a broad community of stakeholders actively participating in knowledge sharing, best practice sharing and discussions on the latest election security technology and procedures. Some examples include:

- **Department of Homeland Security** – Hart is a founding member of the DHS Sector Coordinating Council, a formalized group of industry representatives who together act as a voice on election cybersecurity. In coordination with the DHS Government Coordinating Council, Hart participates in identifying potential security risks and implementing measures to eliminate those risks.
- **Center for Internet Security** – Hart contributed to CIS's recent publication, "A Handbook for Elections Infrastructure Security" and we are engaging in the various appropriate Information Sharing & Analysis Centers (ISACs).
- **Election Assistance Commission** – Hart meets regularly with the EAC and actively participates in industry-wide initiatives.
- **National Academies of Science, Engineering, and Medicine** – As one of only two manufacturers to appear at the meeting of the NASEM Committee on Science, Technology and Law on the Future of Voting (Denver, Dec. 8, 2017), Hart actively participates in the conversation on technology innovation to safeguard elections.
- **Election Center** – Hart leadership serves on the Security Committee with the Election Center, participating in national conversations about cybersecurity at conferences that include a diverse array of election stakeholders (state and county officials; election administrators; technology and security experts) and at least a dozen of our Hart staff members are certified through the Election Center or are working on certification.
- **National Association of Secretaries of State** – Hart regularly exhibits our technology at NASS events, engages in conferences, attends substantive sessions on election topics – including security – and produces a bi-annual white paper submission.
- **National Association of State Election Directors** – Hart regularly exhibits our technology at NASED events and participates in election security sessions.

To summarize, at Hart InterCivic we are committed to election security, as are all the country's voting system providers. We are actively engaged in the current dialog, and associated actions, about election security as critical infrastructure. We engage through the technologies that we offer, through sharing best practices with our customers and through our firm belief in the sanctity of the vote and in the importance that the American public has confidence that every vote counts.

Thank you for the opportunity to appear before the Committee today, and I look forward to your questions.

U.S. Election Infrastructure Sector Coordinating Council

Testimony to the U.S. Senate Rules Committee Wednesday, July 11, 2018 10:30 AM – 12:00 PM

Mr. Bryan Finney, CEO, Democracy Live, Inc. Homeland Security Elections Coordinating Council Executive Committee

Mr. Chairman, Ranking Member Klobuchar and members of the Committee,

I am here today as the CEO of Democracy Live, a Seattle-based voting technology firm delivering electronic balloting technologies to members of our military, voters living abroad and the 35 million blind and disabled voters who cannot see, hold, or mark a ballot. I also have the honor of being nominated and selected as a founding member of the Homeland Security Elections Sector Executive Committee.

Having been working to help modernize elections technology in this country since the 2000 Gore/Bush election, I have had the opportunity to have spoken with and visited hundreds of local elections offices and polling places over the last two decades. My testimony today is a byproduct of that experience:

As a member of the newly established Elections Sector Coordinating Committee (or SCC), supported by Homeland Security, I would like to report that our Committee has been fully operational since our charter in February 2018. This DHS Sector Committee represents a broad and diverse coalition of more than two dozen companies and nonprofits developing, deploying and supporting elections and voting solutions to meet the needs of our nation's 200 million eligible voters and the thousands of hard working elections administrators across the U.S. In addition, our members are working collaboratively with the U.S. Election Assistance Commission, as well as state and local election offices to ensure secure, stable, scalable and protected elections and voting systems. The SCC, representing the greater elections and voting systems providers, absolutely support the increased focus and attention on the security of our nation's elections systems.

As we know, Foreign attempts to probe government voter information platforms during the presidential campaign were clearly aimed at undermining faith in America's democratic institutions. While the consensus among the intelligence community remains clear that no vote tallies were altered in any way, and there is no hard, proven evidence that any private sector provider was compromised, the existence of foreign threats means that we need to continue to be extremely diligent in protecting our nations critical voting infrastructure and instilling confidence in our U.S. electoral systems.

One key aspect of the SCC's role when it comes to developing secure and resilient technology, is to work with DHS and other government partners to ensure that industry expertise is available

to decision and policy makers at all levels. As the providers and innovators who are developing the tools that run our elections and voting systems, our SCC members routinely serve as trusted partners to State and local elections officials. We often are the "first responders," to incidents, issues and possible threats to our elections systems. This requires working closely with federal, state and local officials to identify, report and respond to incidents (both physical and cyber) that may be happening at any level of the electoral process.

SCC members are prepared to meet the threats and challenges that exist. However, with less than two dozen providers serving the needs of over 6,000 elections localities, representing nearly 200 million voters, expectations must also be aligned: First, existing levels of government investment must correspond and increase to meet the growing threats to the entire electoral system. We also request DHS support the existing public-private partnership model outlined in the National Infrastructure Protection Plan (NIPP). As the inventors, innovators, providers and partners to what is truly the engine of our democracy, it is critical we are engaged at the start of any strategic planning, testing, educating or other security initiatives relating to voting systems.

As this committee considers how to better secure our nation's elections infrastructure, I would encourage your members to remember that voting and tabulation machines, although they get the lion's share of the attention, is only the endpoint of a long process with potentially hundreds of voter touchpoints before that voter casts a ballot. These touchpoints must also be secured. They include voter registration, poll books, election night reporting, mail balloting, which is the fastest growing method of voting, and information about who and what is appearing on your ballot.

Laws and certifications exist that can and should be strengthened to better secure our voting and tabulation systems, but if the information systems are corrupted or manipulated than all the work and resources we put into hardening our voting systems may in the end be negated. In this era of voter bots and social misinformation, more and more voters are turning to their local elections officials for accurate objective information. As it was information systems that were manipulated in the recent Presidential election and not tabulation systems, I would encourage Congress to materially support elections officials to offer secure, objective and accessible voter information that voters can trust.

Finally, we need the help of Congress and other public officials in promoting greater public understanding of how elections technology is designed, tested, certified and secured. In the next few months American voters will head back to the polls. Each election is a test of the strength of our democracy. Voters could truly benefit knowing that no polling place svoting machines are connected to the Internet, the majority of systems produce a voter verified paper trail and almost all voting systems undergoes rigorous independent, 3rd party reviews by federal or state approved testing.

We look forward to being partnered with you on the work ahead, and we welcome your questions.

End of Oral Testimony

Extended Written testimony:

Risk assessments, third-party testing and voluntary blueprint models like the NIST Cybersecurity Framework are key priorities. We are also trying to address the need for increased company capabilities under the U.S. Government's Critical Infrastructure designation and how to meet the demand. Hiring additional IT and security personnel, adding resources and increasing training are key to this function. Companies are designating a qualified Chief Security Officer or Chief Information Security Officer to drive physical and cyber security initiatives, or using their existing CSO/CISO to take on new CI-related initiatives.

SCC members are talking to each other about best practices and ways to validate that they have the necessary resources (in-house or third-party) to fulfill changing expectations around security in the elections ecosystem, which is moving away from a static threat model to one of more dynamic threats. We are also working to ensure that our employees have the necessary levels of cyber hygiene training and awareness that are required to do business in the elections industry.

We are looking to provide guidance for state and local customers regarding sound cyber hygiene practices regarding operation and maintenance of our products, physical security and chain of custody policies. We are also working to make sure that customers understand the legal considerations around licensing agreements and use of third-party security services.

Situational Awareness & Communication

Beyond risk management, SCC members are focusing on situational awareness and communication.

At the federal level, SCC Executive Committee members are in the process of applying for government clearances and gaining access to the Homeland Security Information Network (HSIN) in order to receive and share classified and unclassified information with our government partners. The goal is for our full membership to receive this level of access.

Last week, this Committee also heard about how the Elections Infrastructure Subsector is working to develop an enhanced information-sharing framework for security-related communications. In addition to playing a supporting member role in the newly-formed Elections Infrastructure ISAC, which is designed to serve state and local governments, the SCC has proactively engaged the help of the IT-ISAC to form a trusted information-sharing group for the elections industry.

The goal of the Special Industry Group, or "SIG," is to scale up the sharing that's happening through our companies within the private sector to support what the Center for Cyber and Homeland Security at George Washington University has dubbed a "Super-ISAC" capability. This proactive move helps us not only see elections-specific threats, but also broader IT-focused threats towards critical infrastructure.

Working and learning from peer companies in the IT-ISAC has also allowed our members to better understand the Critical Infrastructure Ecosystem, and how it applies to the private sector. Our

goal is to strengthen the dialogue between government and industry regarding the challenges and benefits of two-way information-sharing, particularly with respect to cyber security incidents and gaps.

Response, Recovery & Resilience

Our final area of focus is response, recover and resilience. New and updated election technology is being built with resilience and auditability in mind. The election solutions that are offered by voting system manufacturers are already certified by an independent, federally-accredited Voting Systems Test Laboratory (VSTL) in order to meet standards promulgated by the U.S. Election Assistance Commission (EAC) in conjunction with the National Institute of Standards and Technology (NIST), as well as specific requirements set forth by individual States. These certified software packages and systems are the only versions allowed to be deployed for voting.

One additional and important aspect of the SCC's role when it comes to developing secure and resilient technology, is to work with DHS and other government partners to ensure that SCC industry expertise is available to policy makers. If we are going to move from election hacking events as PR stunts to true initiatives that public and private representatives of the elections community can support and learn from, such efforts need to account for real-world conditions, including business and legal risks, in addition to technical risk. A number of states have strong models for security testing, and vendors know where and how this work is possible.

The last and final point to make is that security is important, but it's just one of many criteria that exist in the elections industry. Turning ideals like "secure" and "accessible" and "anonymous" into affordable, concrete outcomes at scale is a daunting challenge. This work entails third-party dependencies, legacy requirements, competing priorities, political pressures, conflicting incentives, budget shortfalls and rigorous input and scrutiny from government, media and the public. Companies will need to prioritize security fixes and features against other requirements, and meet customer expectations on tight timelines and even tighter budgets.

Thank you.

Bryan D. Finney, CEO
Democracy Live, Inc.
bryan@democracylive.com
206.465.5636

www.democracylive.com

1201 18TH Street, Suite 210
DENVER, CO, 80202
1.866.654.8683
www.dominionvoting.com

October 27, 2017

The Honorable Ron Wyden
United States Senate
221 Dirksen Senate Office Bldg.
Washington, DC 201510

Dear Senator Wyden:

Thank you for reaching out to Dominion Voting. We are completely committed to your goal of ensuring that Americans are confident in the security and reliability of our nation's voting systems. As a member of the U.S. Senate Select Committee on Intelligence, you have undoubtedly heard the unanimous conclusion of our national intelligence agencies that foreign meddling in the 2016 election cycle did not involve any tampering with voting machines or changes in vote tallies, and that any attempts at "cyber manipulation of the U.S. election system designed to change the outcome of the U.S. election would be detected."[1] As we embark upon new efforts to keep U.S. election infrastructure protected as a matter of national security, our systems must remain secure from sophisticated attacks.

Per your question regarding company-focused cybersecurity incidents, Dominion Voting Systems is not aware of any incidents in which an attacker has gained unauthorized access to our internal systems, corporate data or customer data. Additionally, we have not received any information from the U.S. Department of Homeland Security (DHS) or the Federal Bureau of Investigation (FBI) pertaining to any successful cyber intrusions of our systems. If such an incident were to occur, company practices would prioritize notification of our government customers and law enforcement, as appropriate.

Dominion Voting recognizes that maintaining our company security posture – as well as our longstanding record of providing safe, reliable and transparent voting systems – requires constant vigilance and engagement. Our company is using in-house experts, third party private security providers and government partners at all levels to meet existing cybersecurity threats, and to bolster our companywide commitment to risk awareness and sound cyber hygiene practices.

Together with the jurisdictions that we serve, Dominion Voting regularly works with independent, third-party firms to review the security of our company's IT infrastructure. While we have many employees who play a role in company security, our Director of IT, EVP of Engineering and others currently lead our cybersecurity and risk mitigation efforts. In addition to the strict federal and state-level certification processes to which our systems are subjected, we conduct internal and external cybersecurity reviews and risk mitigations, including during the run-up to the 2016 election cycle, and we plan to continue these efforts throughout coming election cycles. We also actively work together with our Election Administrators in discussing concepts for new ways to conduct penetration testing and audits of both our systems and our products in order to build upon past efforts.

For the 2018 cycle and beyond, we are proactively working to enhance our information security program standards, policies and controls by utilizing the National Institute of Standards and Technology (NIST)

[1] (U) National Intelligence Council, ICA 2017-01, 5 January 2017, (U) Assessing Russian Activities and Intentions in Recent U.S. Elections. See also testimony of U.S. Homeland Security Infrastructure & Analysis Cyber Division Acting Director Dr. Samuel Liles before the U.S. Senate Select Committee on Intelligence, 21 June 2017.

DOMINION VOTING

1201 18TH Street, Suite 210
DENVER, CO, 80202
1.866.654.8683
www.dominionvoting.com

Framework for Improving Critical Infrastructure Cybersecurity ("NIST Cybersecurity Framework"). The EAC began promoting the voluntary application of this Framework to elections in February/March 2017, following the DHS critical infrastructure designation for election infrastructure. We are also reviewing the new NICE Framework (NIST Specialty Publication 800-101) and its corresponding Cybersecurity Workforce Development Toolkit as supporting resources for meeting our cybersecurity personnel goals and building upon the comprehensive operational and incident response plan that we developed for the 2016 cycle.

Given the evolving nature of election threats during each cycle, we are actively working with the Election Administrators who currently deploy our systems to enhance protocols for protecting security sensitive critical infrastructure information (CII) and assets from persistent threat actors. The first planned meeting between election industry representatives and DHS is tentatively scheduled for December 2017, and we are hopeful that this working group will be highly effective in furthering the ability of our Election Administrators in keeping our elections safe, transparent and accurate.

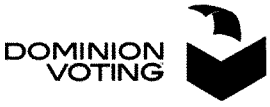
Regarding your questions about unsolicited vulnerability reports, access to voting machines in the U.S. is strictly limited and controlled by the Election Administrators who are entrusted with conducting elections, with violations subject to criminal prosecution under law. States govern this process and establish their policies for controlled access. We recommend that you consult with election officials for a thorough understanding of existing state and local processes for limiting unsolicited access to voting systems, and why such security protections exist. The National Association of Secretaries of State (NASS) and the National Association of State Election Directors (NASED) can be helpful in this regard.

Additionally, since the U.S. Election Assistance Commission (EAC) and state governments play a significant oversight role in the testing and certification of voting systems, we recommend that you speak with these entities to understand how such processes work to identify vulnerabilities and address technical issues before voting systems can be used. Under the Help America Vote Act of 2002, the EAC is tasked with working with NIST to develop Voluntary Voting Systems Guidelines (VVSG) for voting systems. Dominion Voting continues to be an active participant in EAC working groups supporting the VVSG 2.0 effort to build on security-by-design principles for increased transparency and auditability in federal voting system standards. Specific to cybersecurity, industry standards already require election equipment to be used in a closed, private network, with multiple security layers across all components of such systems.

Again, Dominion Voting Systems is deeply committed to the security of our company and its products and we thank you for your efforts to promote public confidence in U.S. elections. Please feel free to reach out to Kay Stimson, our Vice President of Government Affairs, if you need further assistance. Your staff has been provided with her contact information.

Sincerely,

John Poulos
President & Chief Executive Officer
Dominion Voting Systems



1201 18TH Street, Suite 210
DENVER, CO, 80202
1.866.654.8683
www.dominionvoting.com

March 13, 2017

The Honorable Amy Klobuchar
United States Senate
302 Hart Senate Office Bldg.
Washington, DC 20510

The Honorable Jeanne Shaheen
United States Senate
506 Senate Office Bldg.
Washington, DC 20510

Dear Senators Klobuchar and Shaheen:

Thank you for reaching out to Dominion Voting Systems. We appreciate the opportunity to share information with you regarding the security of our systems.

Dominion Voting has not been asked – nor have we voluntarily shared – any product source code or other sensitive, proprietary information with the Russian government. Our company has not had any business dealings with the Russian Federation. Additionally, we are not aware of any product-related risks or vulnerabilities resulting from third-party software programs being shared with Russian authorities. When the U.S. federal government moves to legally exclude vendors (i.e. Kaspersky Labs) from technology systems based on national security risks, we follow suit.

Our company continuously provides enhancements to its voting systems, conducting extensive internal testing of new software to evaluate the functionality, accuracy and security of code. All systems are certified by an independent Voting Systems Test Laboratory (VSTL) in order to meet standards promulgated by the U.S. Election Assistance Commission (EAC), as well as requirements set forth by individual States. These certified software packages are the only versions allowed to be deployed for voting.

At the development level, we are focused on leveraging product features such as encryption, multi-factor authentication, password and trusted user protections, secure locks/seals and secure transmission methods to harden our systems. We have also removed or disabled applications, services and ports that are unnecessary for secure operation of the system, thereby decreasing attack vectors.

Most notably, Dominion Voting's Democracy Suite system provides industry best audit capabilities, with full cast vote record export and adjudicated results reporting. This system was successfully used by the State of Colorado with a 99.999999999% accuracy rate in the nation's first statewide Risk Limiting Audit following the 2016 presidential election.

DOMINION VOTING

1201 18TH Street, Suite 210
DENVER, CO, 80202
1.866.654.8683
www.dominionvoting.com

In addition to hiring a Chief Security Officer to oversee all cyber and physical aspects of company security, we are actively working with the U.S. Department of Homeland Security (DHS) to obtain and share credible threat intelligence information to secure U.S. election infrastructure against nation-state threats. This collaboration is critical for understanding the dynamic threat environment around elections and additional steps that we can take as a company to thwart malicious foreign attacks.

Please note: In a March 9th (2018) open letter to American voters, the Election Infrastructure Subsector Government Coordinating Council (EIS-GCC), which includes members from DHS, the EAC, the National Association of Secretaries of State, the National Association of State Election Directors, the Election Center and the International Association of Government Officials, stated, "Notably, the U.S. Department of Homeland Security (DHS), has said repeatedly that the types of systems Russian actors targeted were NOT involved in vote tallying. Vote tallying systems have a lower cyber-risk profile than the other connected systems we rely upon to bring voters information and services."

While we have no indication from the U.S. intelligence community of any specific foreign targeting against our company or its systems, we will continue to pursue measures that protect our voting systems and their associated software.

Dominion Voting Systems is deeply committed to the security of our company and its products. We welcome the opportunity to educate you and your staff about industry security practices and our systems. If you would like to discuss anything further, please reach out to our Government Affairs team for assistance.

Sincerely,

John Poulos
President & Chief Executive Officer
Dominion Voting Systems

Senate Committee on Rules and Administration
Election Security Preparations: Federal and Vendor Perspectives
July 11, 2018
Questions for the record
Commissioners Thomas Hicks and Christy McCormick

Senator Wicker

Under the Help America Vote Act, the Election Assistance Commission was tasked with developing federal guidelines for local jurisdictions to assist with election security.

1) ***Last year, the Election Assistance Commission developed updated Voluntary Voting System Guidelines, also known as, VVSG 2.0. When developing these guidelines, what factors did the Commission take into consideration when dealing with different localities? Or, asked another way, what different factors, if any, did the Commission consider between rural and urban voting districts?***

   The Voluntary Voting System Guidelines (VVSG) are established standards consisting of a set of specifications and requirements against which voting systems are tested. The specifications and requirements provide factors that focus on basic functionality, accessibility, and security capabilities, which are relevant to all jurisdictions regardless of size or location. The physical location of where a voting system may be deployed is of no consequence in whether a voting system meets the minimum standards of the VVSG. As such, whether a system is used in a rural or urban voting district also plays no part in the certification of a voting system. The EAC does, however, develop the VVSG with input from public working groups in order to facilitate input from all who wish to participate, including those in both rural and urban voting districts.

2) ***How is the Election Assistance Commission working with states to leverage federal resources as they update their systems?***

   The EAC has worked to help states leverage federal resources as they update their systems through its work in support of the recently appropriated $380 million in HAVA Funds, as well as through the EAC's ongoing mission to provide a robust national clearinghouse of election administration information that promotes the effective administration of federal elections.

   As states and territories work to update their systems using the recently appropriated HAVA funds, the EAC has continued to fulfill its role of administering the funds and providing information that ensures states and territories spend the funds within the boundaries established by law. Following this most recent appropriation, the EAC posted answers to Frequently Asked Questions on its website to clarify potential uses of the HAVA funds. In addition, the Commission's grants division conducted several webcasts and teleconference calls with the states to further discuss potential uses for the federal funds. EAC staff has also continuously engaged in one-on-one telephone calls with states and counties seeking answers to specific questions. In addition, because the Commission recognizes that states and territories often find their best new ideas from exchanges with their peers across the nation, the EAC is in the process of publicly sharing the narrative and grant budgets received from each HAVA grant

recipient in hopes that the peer review will assist jurisdictions as they work to fine-tune or identify new projects and activities that will enhance their own election security.

These grant-specific efforts complement the Commission's ongoing efforts to work directly with states to answer questions and provided information about topics such as best practices on how to update election systems and requirements that must be met regarding accessibility, security and other vital topics.

Beyond the Commission's service as the nation's foremost clearinghouse for election administration information, the EAC also serves on the Election Infrastructure Subsector Government Coordinating Council (EIS-GCC), including on its executive committee, established as part of the Department of Homeland Security's (DHS) effort to establish federal elections as part of the nation's critical infrastructure. Through this role, the EAC helps craft and distribute resources that guide election officials working to upgrade the security of their systems. In fact, with the deadline for all states to submit brief security and election improvement plans related to the $380 million in HAVA Fund appropriation, the EAC is planning to soon launch an extensive outreach campaign highlighting best practices in the use of these funds. The EAC has also worked with DHS to advise county officials to communicate with their state IT counterparts, who can provide guidance and information about what direct assistance the state provides for local leaders. These efforts help increase cyber resilience within each election jurisdiction, state, and the nation as a whole.

3) ***FOLLOW-UP: Can you commit to working with local and state officials in rural states to help them access federal resources for modernizing their election infrastructure and securing voter data?***

Yes, the EAC is committed to continuing its work with officials in both rural and urban jurisdictions to assist with securing voting systems. The EAC provides election officials with timely information and best practices that comport with their population and size.

Senator Udall

1) ***Post-election audits have been found to be one of the best tools available to ensure that if systems have been compromised, votes cast have been counted accurately. What is your position on the need for these audits? How many states currently conduct these audits?***

The EAC recognizes the importance of post-election audits to confirm that voting systems are tabulating votes properly and accurately. This is a viewpoint that is widely shared among state and local election officials. The EAC works to provide opportunities for state and local election leaders to discuss audits – both about the value of these activities and the specifics of various audit methods. The Commission has also created audit-related resources and programming to assist election leaders, including:

- "Six Tips for Conducting Election Audits from the EAC" – This resource was created in collaboration with local election officials who helped the Commission develop a series of helpful tips for election management. These tips and recommended best practices

about how to run efficient and effective elections are then distributed and published on the EAC's website.

- "Risk Limiting Audits – Practical Application" – This recently released white paper was authored by a member of the EAC's staff who is one of the nation's most respected authorities on the topic.
- The EAC has conducted auditing workshops at the state level to provide states with information about various types of audits. Just this month, we presented on this topic in a Virginia jurisdiction that is exploring the possibility of implementing risk limiting audits.

2) ***In states that are either fully or partially utilizing Direct Recording Electronic devices – or "black box" voting machines – is the $380 million in HAVA funding that was awarded enough to allow those states to replace that existing equipment with voter-verifiable paper ballot technology like what is used in New Mexico? If not, how much additional funding is needed?***

The $380 million in newly appropriated HAVA funds is not enough to replace existing voting systems with voter-verified paper ballot voting systems. With regard to the amount of funding it would take to replace systems in each state, that question is best answered by polling the states; some public estimates have put the funding amount needed to be between $500 million and $1 billion.

3) ***In last month's Rules Committee hearing to get the state and local perspective on these issues, Missouri Secretary of State Jay Ashcroft, stated that, "The evidence indicates that voter fraud is an exponentially greater threat than hacking of election equipment." Do you agree with his statement? If so, what evidence backs up this claim***?

The EAC is not in a position to expand upon Secretary Ashcroft's comments. However, any interference that could potentially disrupt voter confidence and election outcomes, whether from nation-state adversaries or domestic illegal activity, is something election officials face regularly. Election officials across the nation know that they can't pick and choose the threats they face. They must prepare for every challenge that could impact the integrity of elections, including issues such as those named in this question. It is the EAC's perspective that the nation should work to protect itself against all threats to the integrity of our elections.

Senator Warner

1) ***States now have $380 million in grants to improve their election infrastructure. At the same time, it can be difficult – even for large enterprises – to evaluate the marketing claims of cybersecurity companies and choose products and services that best meet their needs.***

What resources do state election officials have to evaluate cybersecurity product and service vendors?

The Department of Homeland Security offers several free services to assist states and local election officials wishing to assess their security vulnerabilities. The EAC has assisted DHS in

distributing information regarding cyber protections through the EIS-GCC, and before the EIS-GCC was formally chartered, the EAC gathered various vendors and non-profit organizations to create a matrix of services available to election officials. This document was posted with other resources on the EAC website and will be updated through activity of an EIS-GCC working group, which the EAC is co-chairing. Additionally, state election officials are engaging with their Chief State Information Officers to assist with threat assessments and protections.

The EIS-GCC and the Sector Specific Coordinating Council (SCC) continue to work collaboratively to communicate the protections provided under the umbrella of the Critical Infrastructure designation. Through this process, we believe resources to support this critical element of security are now more readily identifiable and available to election officials. We also are committed to working with our partners to identify and add additional resources moving forward.

Would it be helpful for DHS or the EAC to provide a clearinghouse of information, with vetting of vendors?

One of the EAC's statutory mandates is to serve as the nation's clearinghouse of election administration information. This includes information regarding election systems and the vendors that build and provide them. The nation has thousands of semi-autonomous election jurisdictions, and this clearinghouse function helps them learn from one another instead of continually "reinventing the wheel" for each new issue. The EAC firmly believes that this charge is as important and helpful today as it was when the agency was established in 2002. As such, we are discussing with DHS, the EIS-GCC, and the SCC about how to support election officials in vetting vendors who propose to offer cyber security services to the industry.

Is this a function that's being successfully served by the so-called 'cyber navigators' and cyber liaisons?

It is our general understanding that cyber navigators and liaisons are proposed technical personnel at the state and local level who have specialized Information Technology expertise that can assist an election official with technical support and the vetting of contracts. These are ad hoc solutions developed by some states, using HAVA Fund resources.

Is EAC requiring states to spend the $380M on specific cybersecurity improvements? Is it recommending that states prioritize specific improvements?

Congress appropriated the $380M as grants under Section 101 of the Help America Vote Act, and, as such, the EAC is required to follow the statutory language regarding allowable uses contained in section 101. Section 101 does not require that states spend funds on cybersecurity improvements only. At the same time, the EAC is also aware of the Congressional statements regarding preferred uses for the funds. We have provided grant recipients with the report language of the 2018 Omnibus Appropriations Act. In that language, Congress advised the states how it envisioned the funds would be spent, including that states should prioritize their spending to improve and enhance the security of their election processes.

Senator Cortez Masto

1) ***How long is the average time it takes to certify a vendor?***

It is important to note that under the Help America Vote Act, the EAC certifies voting systems as conforming to the Voluntary Voting System Guidelines. The EAC does not certify vendors. Under the Certification Program, a manufacturer of a voting system is required to register with the EAC prior to participation; however, this registration is not a certification of the vendor. The registration provides the EAC with needed information about the vendor and requires the manufacturer to agree to the requirements of the Certification Program.

On average, it takes the EAC approximately eight to 12 months to certify a newly submitted voting system. This amount of time depends on whether a system is being submitted to the EAC for an initial certification or for an upgrade. If the system has already been certified and the vendor is making an upgrade or revising a component, it may take as little as a few weeks or as much as six months to upgrade or change.

2) ***How many vendors receive certification and how many vendors are not certified?***

Currently, there are 18 vendors registered with the EAC as voting system manufacturers. Of these 18 vendors, six have voting systems that are certified under VVSG 1.0.

3) ***Do you think any changes need to occur in order to make certification more accessible and widespread***

The EAC's certification program is readily accessible to any vendor that has completed the manufacturing of a voting system and is registered with the EAC. While the certification program is and should remain accessible, the certification standards and testing processes must remain robust to ensure that the EAC is helping the nation administer its elections with systems that are secure, accessible, and functional. To this end, the ability of a system to make it through the certification process is directly related to how the system is built, its functionality, and whether it meets the minimum standards of the VVSG. The latest iteration of the VVSG 2.0 has been drafted to allow for the most up-to-date and latest trends in technology to be tested against minimum standards. Unfortunately, VVSG 2.0 has not been adopted at this time due to a loss of quorum on the Commission. Once a quorum is reestablished, the Commission will be in a position to adopt the new standards, which may precipitate the entry of new manufacturers into the market place.

Senate Committee on Rules and Administration
Election Security Preparations: Federal and Vendor Perspectives
July 11, 2018
Questions for the record
Mr. Charles Romine

Senator Udall

1) **Post-election audits have been found to be one of the best tools available to ensure that if systems have been compromised, votes cast have been counted accurately. What is your position on the need for these audits? How many states currently conduct these audits?**

NIST Response:

NIST believes that post-election audits are very important. In order to confirm that the results of an election are accurate, audits depend on a trail of evidence. In the draft Voluntary Voting System Guidelines (VVSG) 2.0, currently under development, there are requirements for both the generation of an evidence trail and support for audits. NIST is aware of some states that conduct new statistically backed risk-limiting audits, such as Colorado, but we have not surveyed all states.

Senate Committee on Rules and Administration
Election Security Preparations: Federal and Vendor Perspectives
July 11, 2018
Questions for the record
Mr. Charles Romine

Senator Warner

1) **States now have $380 million in grants to improve their election infrastructure. At the same time, it can be difficult – even for large enterprises – to evaluate the marketing claims of cybersecurity companies and choose products and services that best meet their needs.**

   What resources do state election officials have to evaluate cybersecurity product and service vendors?

NIST Response:

NIST's cybersecurity program provides the foundation for our security guidelines for voting systems. NIST has an extensive set of general cybersecurity guidelines, which are used by federal agencies and can be voluntarily adopted by private industry to secure their information systems. These guidelines address technical, operational, and managerial security controls to help organizations better understand, manage, and reduce their cybersecurity risks. All of NIST's cybersecurity guidelines are freely available on the NIST website. State and local election officials can use all of these resources to help secure their election systems. Some of these guidelines have been incorporated into the Election Assistance Commission's Voluntary Voting System Guidelines security requirements, such as technical guidelines on access control and cryptography.

While NIST's cybersecurity research regarding threats, technologies, and best practices is broadly applicable to election systems, these systems have unique security considerations due to their specific security and privacy objectives, the technologies used, and the environment in which they are used. Guidelines for voting system security must take these unique considerations into account, while also ensuring that other important objectives can be met, including usability, accessibility, interoperability, and cost-effectiveness.

In addition, NIST is an ex-officio member of the Election Infrastructure Government Coordinating Council (EI-GCC). As a member of the EI-GCC NIST is working with DHS, EAC, state and local election officials to identify areas of risk and create best practices and information to mitigate those risks. For example, NIST is co-leading a working group of the EI-GCC with DHS to apply the NIST cyber security framework to the election space. When completed this framework will support election officials, in the same way it has other areas of critical infrastructure, with making good risk-based decisions with regard to their operations and supporting technology.

Senate Committee on Rules and Administration
Election Security Preparations: Federal and Vendor Perspectives
July 11, 2018
Questions for the record
Mr. Charles Romine

Senator Cortez Masto

1) **Can you describe the testing process that takes place at the EAC-accredited labs when it comes to cybersecurity of voting systems?**

NIST Response:

NIST is responsible, under Section 231 of the Help America Vote Act (Public Law 107-252, codified in relevant part at 52 U.S.C. § 20971), for recommending voting system testing laboratories to the Election Assistance Commission (EAC) for consideration in their voting system testing and certification program. NIST uses its National Voluntary Laboratory Assessment Program (NVLAP) to perform the required laboratory assessment.

The Voting System Test Laboratories (VSTLs) are currently accredited to inspect voting systems that are developed to meet the requirements in the EAC's Voluntary Voting System Guidelines (VVSG) 1.0 and 1.1. Currently, manufacturers are developing voting equipment only to the VVSG 1.0 and are waiting for the next VVSG instead of developing to meet VVSG 1.1. Since publication of VVSG 1.0, many new cybersecurity threats have arisen that are outside of the VSTLs scope of testing. With that in mind, NVLAP does its best to ensure that the VSTLs have staff with training and expertise to test for today's threat scenarios so that the labs are able to diagnose serious security issues outside of the scope of VVSG 1.0 and to notify the manufacturer. The labs often are used by individual states for state-specific testing as well. While state-specific testing is outside of the NVLAP accreditation, NVLAP wants labs to have the ability to test for current threats.

The VSTLs, in their security testing, include an inspection of all documentation, functional testing of security-related items, and source code review. The labs test for known vulnerabilities such as those documented by the DHS National Cybersecurity and Communications Integration Center and other similar organizations, as well as those having to do with physical security, such as improperly-protected ports or locks. The VSTLs have incorporated penetration testing into their procedures and have employed security staff with up-to-date security testing and ethical hacking qualifications.

Question#:	1
Topic:	Post-election Audits
Hearing:	Election Security Preparations: Federal and Vendor Perspectives
Primary:	The Honorable Tom Udall
Committee:	RULES (SENATE)

Senate Committee on Rules and Administration
Election Security Preparations: Federal and Vendor Perspectives
Post-election Audits
July 11, 2018
Questions for the record
Mr. Matthew Masterson

Senator Udall

Question: Post-election audits have been found to be one of the best tools available to ensure that if systems have been compromised, votes cast have been counted accurately. What is your position on the need for these audits? How many states currently conduct these audits?

Response: The Department of Homeland Security (DHS) recognizes the importance of auditability of election systems as a best practice. Post-election audits are one of the multiple checks and redundancies in U.S. election infrastructure—including diversity of systems, non-Internet connected voting machines, pre-election testing, and processes for media, campaign, and election officials to check, audit, and validate results— that make it likely that cyber manipulation of U.S. election systems intended to change the outcome of a national election would be detected.

Additionally, the Department supports the work of election officials on the Election Infrastructure Government Coordinating Council, who worked to develop voluntary funding guidance for use of the funds provided to election officials by the Election Assistance Commission (EAC) through the Fiscal Year 2018 Appropriations Acts. Auditability is a core part of this guidance document.

The Department has worked with the EAC on information related to investing in and maintaining election systems. Given their expertise, the Department defers to the EAC to provide a more comprehensive answer on how many states currently conduct audits.

Question#:	2
Topic:	Replacing the Black Box Voting Machines
Hearing:	Election Security Preparations: Federal and Vendor Perspectives
Primary:	The Honorable Tom Udall
Committee:	RULES (SENATE)

Senate Committee on Rules and Administration
Election Security Preparations: Federal and Vendor Perspectives
Replacing the Black Box Voting Machines
July 11, 2018
Questions for the record
Mr. Matthew Masterson

Senator Udall

Question: In states that are either fully or partially utilizing Direct Recording Electronic devices - or "black box" voting machines - is the $380 million in HAVA funding that was awarded enough to allow those states to replace that existing equipment with voter-verifiable paper ballot technology like what is used in New Mexico? If not, how much additional funding is needed?

Response: The $380 million was appropriated to the EAC. As such, the Department defers to the EAC on the purposes for which the funding was used by states, as well as the amount of additional funding that would be required to replace existing equipment.

Question#:	3
Topic:	Voter Fraud
Hearing:	Election Security Preparations: Federal and Vendor Perspectives
Primary:	The Honorable Tom Udall
Committee:	RULES (SENATE)

Senate Committee on Rules and Administration
Election Security Preparations: Federal and Vendor Perspectives
Voter Fraud
July 11, 2018
Questions for the record
Mr. Matthew Masterson

Question: In last month's Rules Committee hearing to get the state and local perspective on these issues, Missouri Secretary of State Jay Ashcroft, stated that, "The evidence indicates that voter fraud is an exponentially greater threat than hacking of election equipment." Do you agree with his statement? If so, what evidence backs up this claim?

Response: The U.S. Department of Homeland Security does not investigate cases of voter fraud. When voter fraud violates federal law, these crimes are investigated and prosecuted by the U.S. Department of Justice. As such, DHS defers to DOJ.

Question#:	4
Topic:	Long-term Costs Recommendations
Hearing:	Election Security Preparations: Federal and Vendor Perspectives
Primary:	The Honorable Catherine Cortez Masto
Committee:	RULES (SENATE)

Senate Committee on Rules and Administration
Election Security Preparations: Federal and Vendor Perspectives
Long-term Costs Recommendations
July 11, 2018
Questions for the record
Mr. Matthew Masterson

Senator Cortez Masto

Question: What advice or recommendations do you have for states that are making upgrades and investments in their voter systems are concerned about the long-term costs of their upkeep?

Response: The Department has worked with the EAC on information related to investing in and maintaining election systems. Given their expertise on the purchase, procurement, and management of voting systems, the Department defers to the EAC to provide a more comprehensive answer.

Question#:	5
Topic:	RVAs
Hearing:	Election Security Preparations: Federal and Vendor Perspectives
Primary:	The Honorable Catherine Cortez Masto
Committee:	RULES (SENATE)

Senate Committee on Rules and Administration
Election Security Preparations: Federal and Vendor Perspectives
RVAs
July 11, 2018
Questions for the record
Mr. Matthew Masterson

Senator Cortez Masto

Question: Which states have asked for and received a risk and vulnerability assessments on their election systems?

Response: We are working hard to ensure all states that have requested risk and vulnerability assessments on their election systems receive them without delay. While we do not identify the entities that voluntarily request specific services, DHS has conducted a number of risk and vulnerability assessments for election stakeholders this year. In addition, DHS is providing regular vulnerability scanning that includes recommended mitigation to an even larger number of stakeholders.

Question#:	6
Topic:	Misinformation Campaigns
Hearing:	Election Security Preparations: Federal and Vendor Perspectives
Primary:	The Honorable Catherine Cortez Masto
Committee:	RULES (SENATE)

Question: We are now learning that the dissemination of misinformation by malicious actors, including Russia, through social media attempted to sway voters and influence the 2016 election. Can you describe the Department of Homeland Security's efforts to prevent and address these misinformation campaigns on social media for the next election?

Are you working with the EAC on these information operations? Please describe your efforts.

Are you working with state and local officials who might become aware of these misinformation campaigns? Please describe your efforts.

Response: The Department has organized to counter foreign interference in partnership with the Federal Bureau of Investigation (FBI), the intelligence community, and others. While the FBI's Countering Foreign Interference Task Force is leading domestic response efforts, DHS is working to increase resilience to Foreign Interference operations. To achieve this, DHS is raising awareness by providing, in coordination with the FBI, briefings to key stakeholders, with a focus on state and local election officials.

Question#:	7
Topic:	Security Clearances
Hearing:	Election Security Preparations: Federal and Vendor Perspectives
Primary:	The Honorable Catherine Cortez Masto
Committee:	RULES (SENATE)

Question: You stated in your written testimony that DHS is working with state chief election officials and other election staff to provide them with security clearances. How quickly is this process moving forward?

Response: DHS prioritizes the processing of security clearances for election officials. Each State Chief Election Official has been extended the opportunity to apply for a security clearance, as well as two additional personnel on their staffs. A significant number of those have been granted security clearance and we will continue to process additional clearances as they are requested by the states. In addition to security clearances, we have leveraged other tools, such as one-day read-ins to provide classified information to election officials who lacked clearances when appropriate.

Question#:	8
Topic:	Disseminating Information
Hearing:	Election Security Preparations: Federal and Vendor Perspectives
Primary:	The Honorable Catherine Cortez Masto
Committee:	RULES (SENATE)

Question: What challenges are you facing ensuring that information gets to the people who need it?

Response: DHS leads efforts to defend our nation's critical infrastructure from cyber threats. Today's infrastructure is more complex and dynamic with interdependencies that increase the challenge of reducing risk and ensuring resiliency. DHS remains committed to working with our interagency partners to share every piece of information available. As new threats emerge, we are redoubling and adapting our information sharing efforts. DHS not only shares unclassified and classified cyber threat information as well as providing a full range of technical assistance capabilities, but also closely coordinates with our federal partners, including intelligence agencies, law enforcement, and sector-specific agencies to share as much information as possible.

Senate Committee on Rules and Administration
Election Security Preparations: Federal and Vendor Perspectives
July 11, 2018
Questions for the record
Mr. Scott Leiendecker

Senator Udall

1) Can states that do not replace their Direct Recording Electronic devices – or "black box" voting machines actually conduct post-election audits and make such accuracy guarantees to their voters?

   My company, KNOWiNK, focuses almost exclusively on electronic poll books, which is verifying the individual voter when they check into their polling place and is not associated with voting machines or voter tabulation. However, our PollPad product helps election authorities with the certification process, making it easier for election workers to audit and account for Election Day activities, but does not deal with the tabulation side.

2) In the hearing this committee held last month to hear from state and local officials on these issues, Missouri Secretary of State Jay Ashcroft, stated that, "The evidence indicates that voter fraud is an exponentially greater threat than hacking of election equipment." Do you agree with his statement? If so, what evidence backs up this claim?

   KNOWiNK has always made election security our highest priority. Our system provides more accurate and up-to-date voter records, which helps prevent individuals from attempting to vote more than once in an election.

   I was appointed Election Director for St. Louis City in 2005. You may recall that St. Louis City had significant issues with their election in 2000 and our team was constantly working to restore the integrity of our election authority. As Election Director, I personally witnessed people who committed or attempted to commit voter fraud and voter absentee fraud, and we referred those cases to the U.S. Attorney where they were prosecuted. While these cases of voter fraud were not widespread, election authorities must be vigilant and do everything possible to prevent voter fraud and the integrity of election equipment.

3) The intelligence community is warning us that Russia—and maybe others—will try to interfere in our elections again. We know hackers in Russia accessed multiple state election systems in the past. Are our state election systems secure? What actions should states be taking now that many are not already taking?

   There is always room for improvement. States should be taking full advantage with what the Department of Homeland Security and the federal government has done to provide funding and resources to ensure our elections are secure. They need to update their voter registration systems in counties and states. These systems are often very outdated and don't utilize the resources available to them or the systems that they do have to their greatest ability. Making sure that systems are updated to the most current operating systems, which sounds intuitive,

but I am constantly surprised how many election authorities are using old operating systems, which can leave their systems vulnerable to attack.

KNOWiNK leverages some of the top companies like Apple and AWS to secure our systems. We send our systems through a rigorous penetration testing annually and our equipment has been subject to numerous certification standards in many states and we believe our systems are built not only to standard, but well above the required standards.

Senator Warner

1) Competition drives innovation and better product quality. For competition to work, it's also important for buyers to be able to effectively evaluate the quality of what they're buying.

   If an election agency that has bought voting systems from you wants to have those systems tested by independent security experts, is there anything in your sales or service agreements that would prohibit that?

   No, and we encourage this testing.

   Will you commit to allowing election agencies to procure independent security testing?

   Yes, in fact, in your home state of Virginia the state elections commission requested us to present our equipment to the Virginia Information Technologies Agency (VITA) to face their rigorous security standards. We welcomed this challenge and passed the test. These tests make our company better, and are one of the reasons we believe our electronic poll book is the best and most secure on the market.

   Do your systems rely on any hard-coded credentials for authentication, remote access, or remote diagnostics?

   No on all three.

2) We have heard complaints of vendor lock-in from localities in Virginia, who point to long-term service contracts with highly variable and opaque pricing, and restrictions on third-party servicing.

   Do your products support common data standards, formats and protocols to facilitate interoperability with other vendors' products and services?

   Yes. We are one of the most versatile elections solutions on the market and work seamlessly with every voter tabulation company. We leverage the iPad and Swift Programming Language, which are very common. We are constantly updating our code to bring it up to date with the most current programming language. Our contracts are also simple, straight-forward and transparent

Do you support efforts in the revised voting system guidelines to push for greater interoperability?

Yes, we encourage collaboration and this value is already baked in to our company systems.

3) Today, a standard business practice for software and IT providers is to define a product lifecycle and provide the customer with a specific date on which product and security support will cease. This helps prime consumer expectations and facilitates orderly transition to new systems or software.

In your product agreements, do you inform purchasers of the expected end-of-life of a voting system?

We use an off-the-shelf solution with the iPad so it can be difficult to predict end of life with companies like Apple. However, we elected to partner with Apple because of their operating system, which allows users to continually get operating system and hardware updates, which is more affordable for election authorities. For counties that use our product, they have affordable options if a system ever becomes outdated and our systems will continue to be compatible with the iPad product.

Do any of your products rely on beyond-end-of-life third party software like Windows 2000 or XP?

No. We use Apple exclusively.

4) The Copyright Office has the power to create exemptions to the anti-circumvention protections of the Digital Millennium Copyright Act, for instance to provide 'good faith' researchers the ability to evaluate the security of devices.

The Copyright Office's 2015 rulemaking provides an exemption for research on electronic devices, expressly including voting systems.

Does your company have a publicized process in place to receive and respond to vulnerabilities found by third party researchers? How many times in the last five years has your company received such reports?

We are not a voter tabulator, so our process is much different than on the tabulation side, however we proactively do vulnerability tests and welcome any third party to contact us if they have information to share. Zero.

Has your company ever threatened a cybersecurity researcher or an election vendor with legal action arising out of a security assessment?

No.

Senate Committee on Rules and Administration
Election Security Preparations: Federal and Vendor Perspectives
July 11, 2018
Questions for the record
Mr. Peter Lichtenheld

Senator Wicker

Peter Lichtenheld is the Vice President of Operations for Hart InterCivic, the oldest company presenting at the hearing. This question will explore past election security concerns, and the success of federal intervention.

1. Mr. Lichtenheld, Hart InterCivic clearly has a long history in this industry and a wide array of experience. In the past 10 years, how have election hacking attacks been different than the issues we are dealing with today?

   The issues we are dealing with today include attempts to influence the election by interfering not only in areas that are part of our nation's election infrastructure (state voter registration databases) but also in areas *outside* the election infrastructure. From our perspective, what seems new in all this is the activity designed to influence voter behavior and/or reduce their confidence in the broader democratic process. Whether it's hacking and stealing emails from private email servers or using fake social media accounts to share the stolen information or other misinformation designed to influence voters, experts in these areas need to be aware of and working together to mitigate those risks and shut down those attack vectors.

   Within the critical election technology infrastructure, the work that state and local election authorities are doing to harden their defenses is critically important, especially in any areas where vulnerabilities have already been exposed. They are being supported by federal agencies, outside cybersecurity experts and private sector technology partners, including Hart InterCivic. To be clear: voting systems – which is what Hart InterCivic sells and supports – have not been hacked or compromised. That said, we will never let our guard down. We are actively and aggressively "upping our game" – in partnership with government agencies, regulatory bodies and private sector partners that work in the election space.

FOLLOW-UP: Do you think local jurisdictions have the proper expertise to identify and cure election vulnerabilities, or do you think it is necessary for federal mandates and intervention?

While we believe decentralized election management and local control are an important security feature of how elections are run in the United States, we also believe local jurisdictions need additional assistance. The smaller the jurisdiction, the more assistance they need. The work currently happening at the federal level (U.S. Senate and U.S. House of Representatives Committee work, DHS GCC/SCC, EAC, etc.) in partnership with state and local

groups (NASS, NASED, etc.) is an important step in defining guidelines for security best practices, as well as an opportunity to provide the funding needed for state and local election officials to make the necessary investments to help secure our elections.

Senator Udall

1) Can states that do not replace their Direct Recording Electronic devices – or "black box" voting machines actually conduct post-election audits and make such accuracy guarantees to their voters?

Every election administrator, regardless of what kind of voting system they use, has a variety of methods to audit the integrity of the election, and to provide confidence and reassurance to voters. Hart assists all our customers in these areas, with detailed procedures and support for things like: logic and accuracy testing; review and reconciliation of polling place level and centralized reporting assets; and cross-referencing and comparison of ballot-level voter selections with tabulated results.

2) In the hearing this committee held last month to hear from state and local officials on these issues, Missouri Secretary of State Jay Ashcroft, stated that, "The evidence indicates that voter fraud is an exponentially greater threat than hacking of election equipment." Do you agree with his statement? If so, what evidence backs up this claim?

The topic of voter fraud (or any topic related to voter registration or validation of voter registration at the polling place) is far outside the scope of where Hart operates. We have no insight or comment on this topic.

3) The intelligence community is warning us that Russia—and maybe others—will try to interfere in our elections again. We know hackers in Russia accessed multiple state election systems in the past. Are our state election systems secure? What actions should states be taking now that many are not already taking?

Hart supports the work currently being led by the EAC in partnership with DHS to offer and conduct independent cybersecurity audits of each state's election infrastructure, identify potential threat vectors and implement risk mitigation plans. In addition, we support state election office engagement with the EAC, DHS, MS-ISAC and EI-ISAC and encourage state election offices to study the information these groups make available. State election offices should also take appropriate actions to deter, identify and recover from cyberattacks, and state election information offices should share as much information on security best-practices as possible with their local jurisdictions.

Senator Warner

1) Competition drives innovation and better product quality. For competition to work, it's also important for buyers to be able to effectively evaluate the quality of what they're buying.

   If an election agency that has bought voting systems from you wants to have those systems tested by independent security experts, is there anything in your sales or service agreements that would prohibit that?

   Will you commit to allowing election agencies to procure independent security testing?

   [Consolidated response to both questions immediately above.]

   As a normal part of comprehensive federal and state certification processes, all elements of voting systems – including hardware/software security capabilities, source code, auditability, accessibility and more – are thoroughly tested by government-accredited independent test labs. Federal and state authorities rely on the input of these vetted experts when deciding whether to certify a system for use in elections.

   Hart is very supportive of testing and certification processes which hold manufacturers to the highest standards of security, defined by the foremost experts on the topic. We believe those standards – and associated testing – should remain part of the federal and state certification processes.

   If there are concerns among lawmakers, election officials or cybersecurity experts that current federal and state regulatory processes are somehow insufficient, resulting in potential security vulnerabilities, then focus and attention should be placed on updating/improving the existing testing processes, rather than relying on separate, ad hoc testing to try to fill those gaps.

   Do your systems rely on any hard-coded credentials for authentication, remote access, or remote diagnostics?

   Hart's voting systems do not include hard-coded user credentials for authentication. No Hart system has ever included or supported any type of remote access or remote diagnostics software.

2) We have heard complaints of vendor lock-in from localities in Virginia, who point to long-term service contracts with highly variable and opaque pricing, and restrictions on third-party servicing.

   Do your contracts include any restrictions on third-party servicing?

No, none of the above applies to Hart contracts. We have many customers who have third parties service their equipment.

Do your products support common data standards, formats and protocols to facilitate interoperability with other vendors' products and services?

Hart's data export capabilities have been designed with an eye toward the values of transparency, data exchange in common formats, efficiency, and software independence. With that in mind, our systems can export data in common formats suitable for third-party use, outside of our voting systems, including TXT, CSV, PDF, HTML, and XML formats.

Hart also has extensive experience integrating its products with other systems. Hart's design and development team includes experienced application design, engineering, and programming staff to support integration with other systems, and we have managed numerous successful integration projects.

Do you support efforts in the revised voting system guidelines to push for greater interoperability?

Hart supports the definition and utilization of standard data formats to increase transparency and efficiency in election operation. As voter registration data flows from the state to local jurisdictions' pollbook/voter check-in processes; and as election data flows from the state to local jurisdictions' election management systems (EMS); and as tabulated election results data flows from the localities' EMSs into various results reporting systems, the use of transparent and standard data formats helps improve how these disparate systems work together seamlessly. This drives increased quality and speed of election operations, resulting in higher voter confidence.

3) Today, a standard business practice for software and IT providers is to define a product lifecycle and provide the customer with a specific date on which product and security support will cease. This helps prime consumer expectations and facilitates orderly transition to new systems or software.

In your product agreements, do you inform purchasers of the expected end-of-life of a voting system?

We do not specify an end-of-life or end-of-support date for our voting systems because customers who buy the same system at different times should expect to get a similar lifespan from their systems. We typically tell our customers to expect 10-15 years of use from their system. For example, if a customer bought a new system in 2003 and another customer bought the same system in 2006, they should both expect to get 10-15 years of use without that timeline being cut artificially short by an end-of-service date.

Variability in product lifespan is tied to how often jurisdictions have elections and how well they take care of the equipment. Ultimate end-of-lifespan for a system could also be driven by external factors such as changes to federal or state certification requirements or voting laws.

Do any of your products rely on beyond-end-of-life third party software like Windows 2000 or XP?

We do have customers using software components that run on older operating systems. We encourage all election officials using older systems to upgrade to new, modern technology. That refresh process has begun nationally; however, there are still many jurisdictions using older technology. Funding is a major hurdle for many of these jurisdictions still using older generation systems. The funds recently made available ($380M in the Consolidated Appropriations act of 2018) are a good example of government working together at the federal, state and local levels to make the necessary investments in election security.

4) The Copyright Office has the power to create exemptions to the anti-circumvention protections of the Digital Millennium Copyright Act, for instance to provide 'good faith' researchers the ability to evaluate the security of devices.

The Copyright Office's 2015 rulemaking provides an exemption for research on electronic devices, expressly including voting systems.

Mr. Lichtenheld, why has your company urged the Copyright Office to overturn that determination and limit independent security assessments of the nation's voting systems?

As a normal part of comprehensive federal and state certification processes, all elements of voting systems – including hardware/software security capabilities, source code, auditability, accessibility and more – are thoroughly tested by government-accredited independent test labs. Federal and state authorities rely on the input of these vetted experts when deciding whether to certify a system for use in elections.

Hart is very supportive of testing and certification processes which hold manufacturers to the highest standards of security, defined by the foremost experts on the topic. We believe those standards – and associated testing – should remain part of the federal and state certification processes.

If there are concerns among lawmakers, election officials or cybersecurity experts that current federal and state regulatory processes are somehow insufficient, resulting in potential security vulnerabilities, then focus and attention should be placed on updating/improving the existing testing processes, rather than relying on separate ad hoc testing to try to fill those gaps.

Does your company have a publicized process in place to receive and respond to vulnerabilities found by third party researchers? How many times in the last five years has your company received such reports?

Hart cares deeply about election security and we have a strong history of being open to external reviews as part of federal and state certification processes. We remain committed to acting appropriately to address and resolve any questions or concerns that stem from such reviews.

Hart has a process for receiving, reviewing and taking appropriate action on reports generated by third-parties. Going above and beyond the already thorough federal and state testing and review processes, we have commissioned our own independent security review of our latest generation voting system and have incorporated the findings into ongoing system enhancements. We have not received any other unsolicited reports in the past five years.

Has your company ever threatened a cybersecurity researcher or an election vendor with legal action arising out of a security assessment?

No.

Senate Committee on Rules and Administration
Election Security Preparations: Federal and Vendor Perspectives
July 11, 2018
Questions for the record
Mr. Bryan Finney

Senator Wicker

In his testimony, Mr. Finney reminded the committee that voting and tabulation machines are the endpoints for the voting process, which has "potentially hundreds of voter touchpoints" before the ballot is cast. Specifically, he mentions voter registration, poll books, election night reporting, mail balloting, and information about who and what appears on the ballot.

1) Mr. Finney, you mentioned the hundreds of touchpoints in the process of voting; registration, poll books, mail balloting, and more. Looking at the election life cycle, in your opinion, where are states most vulnerable to election attacks?

Response: *As the Chair of the Homeland Security Elections/Voting Sector Emergency Response Task Force and Vice-Chair of the SCC, we as a Committee have spent hundreds of hours reviewing this question. It is perhaps the most important question you can ask. In my opinion, after twenty years working with State and local elections officials across the U.S., the biggest threat to elections security is what happens in the event of a widespread incident, or attack that prevents voters from voting on Election Day. In the event of a widespread natural disaster, domestic terrorist attack at polling locations, or a widespread power outage how do voters vote? What is the Plan B for voting?*

I am deeply concerned that in the event of an incident or attack on Election Day we do not have a "back-up" in the event voters cannot vote on the "first Tuesday after the first Monday in November" as prescribed in Article II of the U.S. Constitution.

2) FOLLOW-UP: Do you see additional needs in rural states vs. urban states in addressing these vulnerabilities? If so, are there specific strategies for addressing the needs of rural vs. urban areas?

Response: *With over 8,000 jurisdictions responsible for the conduct and administration of elections in the United States, there are far more rural localities than urban. Even in "urban" states, there are more rural jurisdictions than urban. Most of the 8,000+ elections administrators across the U.S. have minimal IT security or emergency response training. The Department of Homeland Security and The Cybersecurity and Infrastructure Security Agency (CISA) are currently executing on a plan to help educate and support each of the 8,800 elections offices on tools and support available through DHS and CISA.*

Senator Udall

1) Can states that do not replace their Direct Recording Electronic devices – or "black box" voting machines actually conduct post-election audits and make such accuracy guarantees to their voters?

Response: *The vast majority of 100 million+ voters voting at the 160,000+ voting location in the U.S. will be voting on paper ballots in 2020. The few remaining states and jurisdictions that still vote on all DRE, will be migrating to a paper system in the next few months, or shortly after 2020. Although there has not been any demonstrable proof of any votes being intentionally corrupted, or changed, post-election audits are certainly another layer for voters to trust the security and integrity of elections. I do not believe a pure DRE tabulation system could produce a risk limiting audit.*

2) In the hearing this committee held last month to hear from state and local officials on these issues, Missouri Secretary of State Jay Ashcroft, stated that, "The evidence indicates that voter fraud is an exponentially greater threat than hacking of election equipment." Do you agree with his statement? If so, what evidence backs up this claim?

Response: *Nearly 140 million ballots were cast in 2016 U.S. Presidential election. There were four known cases of voter fraud in that election. There were zero cases of votes being "hacked" in voting equipment. So yes, technically four is higher than zero.*

3) The intelligence community is warning us that Russia—and maybe others—will try to interfere in our elections again. We know hackers in Russia accessed multiple state election systems in the past. Are our state election systems secure? What actions should states be taking now that many are not already taking?

Response: *As a sitting member of the Department of Homeland Security Elections/Voting Sector ExCom (SCC), we review this question on a daily basis. The phrase "hackers in Russia accessed multiple state election systems" is very loose. The term "elections systems" is quite broad. To be clear, nefarious Russian actors scanned a number of State voter registration systems. (Not vote tabulation systems.) Per public disclosures from the Intelligence Community, zero voter registration records were altered in any way by foreign state actors. As there is zero evidence of tabulation systems being attacked, no vote totals were corrupted in any way.*

However, although there is no evidence tabulation systems were corrupted, nor manipulated, there is plenty of evidence Russia targeted and attacked our voter information systems. Via targeted social media misinformation campaigns, millions of voters were misinformed about who and what was on their ballot and their candidate information. Voters are highly susceptible to Facebook, Twitter and other sources of potential misinformation. In my opinion, voter information is the most vulnerable component in the voting process and has the highest chance of impacting an election.

Senator Warner

1) Competition drives innovation and better product quality. For competition to work, it's also important for buyers to be able to effectively evaluate the quality of what they're buying.

   If an election agency that has bought voting systems from you wants to have those systems tested by independent security experts, is there anything in your sales or service agreements that would prohibit that?

Response: *Beyond sitting on the Executive Committee for the Department of Homeland Security Elections/Voting Sector (SCC), I am the founder and CEO of Democracy Live, the largest provider of cloud-based balloting in the U.S. As the CEO of Democracy Live, we welcome and encourage states to do independent testing and bring in 3rd party security analysts. We believe that is a competitive advantage for Democracy Live.*

   Will you commit to allowing election agencies to procure independent security testing?

Response: *Yes. At Democracy Live, we have already undergone independent testing by federally approved lab testing and independent state-level testing. We encourage 3rd party review and testing of our systems.*

   Do your systems rely on any hard-coded credentials for authentication, remote access, or remote diagnostics?

Response: *As a cloud-based (non voting) system, our application resides in the Amazon AWS Secure Cloud. Our systems do offer hard-coded credentials and remote access and diagnostics.*

2) We have heard complaints of vendor lock-in from localities in Virginia, who point to long-term service contracts with highly variable and opaque pricing, and restrictions on third-party servicing.

   Do your products support common data standards, formats and protocols to facilitate interoperability with other vendors' products and services?

Response: *Democracy Live is the only EAC federal lab approved system that has been tested and deployed to work with <u>every</u> major voting system in the U.S. Yes, we interoperate closely with other vendors data systems.*

   Do you support efforts in the revised voting system guidelines to push for greater interoperability?

Response: *As a cloud and polling-place balloting system, we are highly reliant on data integration with other vendors. In order to expand (and allow for) innovation, competition and taxpayer savings, we strong encourage interoperability, especially as it relates to ballot and voter registration data.*

3) Today, a standard business practice for software and IT providers is to define a product lifecycle and provide the customer with a specific date on which product and security support will cease. This helps prime consumer expectations and facilitates orderly transition to new systems or software.

   In your product agreements, do you inform purchasers of the expected end-of-life of a voting system?

   Response: *As a mostly cloud-based system, our agreements are mostly subscription-based and entitle our customers to the most recent upgrades. Where we do not offer a subscription option, yes we do define the end of life cycle in our agreements.*

   Do any of your products rely on beyond-end-of-life third party software like Windows 2000 or XP?

   Response: *No, we do not.*

4) The Copyright Office has the power to create exemptions to the anti-circumvention protections of the Digital Millennium Copyright Act, for instance to provide 'good faith' researchers the ability to evaluate the security of devices.

   The Copyright Office's 2015 rulemaking provides an exemption for research on electronic devices, expressly including voting systems.

   Does your company have a publicized process in place to receive and respond to vulnerabilities found by third party researchers? How many times in the last five years has your company received such reports?

   Response: *No we have not, but will take this under consideration. It may be a competitive advantage to do this and may help strengthen our product line.*

   Has your company ever threatened a cybersecurity researcher or an election vendor with legal action arising out of a security assessment?

   Response: *No we have not. We encourage security assessments and reviews as we believe it makes our system more secure and more competitive in the marketplace.*

○