This text is being provided in a rough draft format. Communication Access Realtime Translation (CART) captioning is provided in order to facilitate communication accessibility and may not be a totally verbatim record of the proceedings.

EAC Election Readiness Summit.
October 3, 2018.

>> Ladies and gentlemen, the event is about to begin. If you could find your seat. Thank you.

>> THOMAS HICKS: Good morning, everyone. My name is Thomas Hicks and I'm chairman of the United States election assistance commission. The commission is honored to host the 2018 election readiness.

Earlier this year they held an all-day summit at the national press club. To highlight the spectrum of states, local issues, and voters would face as they prepared for the 2018 federal election. Now that those elections are a little over a month today, today's event is a little of a bookend to the earlier summit, giving us a chance to revisit some of those same topics and examine where things are now.

Including how states are using the $380 million appropriated earlier this year, and the steps states are taking to improve the security, accessibility, and efficiency of the upcoming elections.

Since the 2016 elections, much of the public discourse has focused around security. And for a good reason.

And while this very public attention to this issue of election security is fairly new, the work to secure elections is not new to election officials, the EAC, or the tens of thousands of election administrators, staff, and election workers who support that work.

It's fair to say that 2016 changed the threat environment we face, hitting state and local election officials against nation-state actors who scan for vulnerabilities and were successful in accessing one state's voter rolls.

These same actors made additional attempts to infiltrate states' elections systems ahead of the 2018 midterms, and by all accounts, they will be back for 2020.

Elections can lead up to the 2018 election midterms, and increasing security and resiliency of their systems informing national and regional relationships to improve information sharing and cyberprotections.

The EAC is proudly serving a lead role in creation of these federal partnerships, and we establish the government coordinating council charged with administrates successful implementation of the federal government's designation of elections as the nation's critical infrastructure.

Today, we'll be exploring a bit of how election officials are working to balance the demands of ensuring election security with the hundreds of facets of their jobs that don't make the headlines, including voter registration, poll worker recruitment, poll work training management, post election audits, using election data to

improve the voters' experience, and so much more. As a reminder, this Friday was the original deadline for the EAC's clears house awards, but since we're getting so much great feedback we're going to attend that out to the end of November.

This year's awards are being named after Brian Louis, and Wendy Noran from Boone County, Missouri. Today's events will take a closer look at the intense year of preparing for the elections around the country who have worked tirelessly.

And they, like the EAC, are committed to ensuring the process is accurate, accessible, and fair to all.

Before we dive in, I have a few housekeeping things to share. And I know most you have heard this before but we're going to do it again. First, if your a social media user, unlike myself, we encourage you to post today's summit using #countdown18 to promote helpful materials for election officials and voters to prepare for the upcoming elections. And most importantly, second, there will be opportunities throughout the day for audience members to ask questions of our panelists. When doing so, we ask three things: One, speak into the microphone so everyone can hear you.

Two, give your name and affiliation.

And three, and most importantly, actually ask a question.

[Laughter.]

Next, if you have a cell phone, or other electronic device, please place your phone on silence. And as many of you already know, we're going to have a vendor event at 2:20, and I've asked the President to give you an announcement at 2:20 to tell you to come back. And if you've read the paper, you know that's a joke, but apparently you folks don't read the paper anymore.

[Laughter.]

And if you need anything throughout the day, ask our staffers, Brenda, raise your hand in the back. David, who's at the table. And Natalie, who's -- no, she's right up front here.

So if you have any questions or need anything, talk to one of those three staffers, and they will be happy to help you in any way they can. Now let's turn to the first panel.

Our first panel takes a closer look at how states and local election leaders are investing in enhancing security, including how they will use their portions of the $380 million in security funds appropriated by Congress earlier this year.

While each of today's panelists has a unique story to tell, all of them are working day and night towards the same goal: Ensuring that voters have confidence, that the elections are secure and accurate. We look forward to highlighting their efforts during the coming hour.

Joining me for the discussion today is Alabama Secretary of State John Merrill, who was first elected to public office as a representative of the House district 62 in 2010. And then elected as Secretary of State in 2014. Since he took office, Alabama has more than one million newly registered voters, setting a new state record for registered voters participating in elections. He is also a National Association of Secretary of State, member of. And member of the Republican association of Secretaries of State. He's cochair of

NASS's voting representation committee and serves on the steering committee for national voter registration day and is a member of the EAC standards board.

Meghan Wolfe is the administrator of Wisconsin's election commission. She joined the state's service as voter services election specialist in 2011. Initially she developed and implemented voter outreach, communication, and resources both on a public information scale and assisting individual voters. Later she led the multiyear effort to launch My Vote Wisconsin so it's easier for voters to use and easier for clerks to assist them. In April of 2017 she became assistant administrator, managing the staff and IT team and the commissions elections security planning. In March, she was -- and serves on the standards board.

Secretary of State Kim Wyman. Elected in 2012 and currently serving in her second term. Prior her current role as secretary, served as the elections counter for nearly a decade.

Secretary Wyman's responsibilities including overseeing elections, corporations, charity filings, the Washington state library, the Washington talking book and Braille library, and the combined fund drive for charitable giving, and -- and Washington's oral history, and exhibit program that tells the states most intriguing stories. Secretary Wyman is a graduate of California State-Long Beach, and holds a master's degree in public administration from Troy State University.

She was awarded an honorary doctorate in the university in Seattle, and the secretary is also a certified elections and registrar administrator.

And Washington State certified election administrator.

We welcome you as well, Secretary.

Last but not least, is Joe Rozell, the election director for Oakland County, and is a certified elections registration administrator certification from Auburn University. He's a member of the election center and the Michigan association of county clerks.

Rozell is an adjunct faculty member of Oakland University, teaching political science and also serves as an elected nonpartisan city commissioner in Huntington Woods, Michigan. Welcome, and I look forward to the discussion.

My first question to each of you, we can all agree that in a different -- we are in different place than we were -- in a different place than we were in 2016. Tell us what steps your state has taken to improve elections this November, and what future investments you plan on making -- to make. Secretary, do you want to start off?

>> JOHN MERRILL: I'm honored to be here and to be a part of this panel this morning to answer some questions that may be generated from the audience, as well as to share with you some of the things that we're doing in the great state of Alabama, regarding ensuring integrity and credibility in the elections process.

We know unless we continue to validate, inform, and make sure that we make comfortable our people about the things that we're facing, especially in the area of cybersecurity, we will lose credibility in their eyes and it will deter participation.

Any time people lose confidence in the process, it's a negative

for all of us, because the validation of the results would not be received as well as it would be otherwise. So we think that it's very important to make sure that we're maintaining that fight, each and every day.

The other thing I think we have to recognize is that this is not something this is just going to be here for a short period of time and move on. So as one of the things we were talking about at our conference in Philadelphia earlier this year, was that two years ago we didn't have any breakout sessions on cybersecurity, and now today, roughly 75% of the things that we talked about at our conference were related to cybersecurity and elections and it's important to know that we have to remain diligent in that regard.

We were doubly excited, we were able to receive that new allocation from the government related to the funds that were recently released. Our contribution was a little bit over $300,000, but the 6.1 million we received was very important to our state. Many of you nay know that our state is not a state that is rich when it comes to resources that are available for discretionary purposes or specifically in this particular area. So anything that we can receive that can help us benefits not only this area, but all the people in our state.

One of the frustrations that I experienced when I became Secretary of State in Alabama three years, nine months, and 14 days ago, was that we had the original HAVA allocation that was set aside and it was divided in our 67 counties by the number of voters in each individual area. One of the things we wanted to make sure that we did was to evaluate where those resources needed to be invested for the greater good of our entire state.

The reason is because we still have some of our 67 counties who have received those resources from 15, 20 years ago that are still in their general fund bank accounts in their local counties. They still have yet to be invested in the elections process, which is not a benefit of anybody. Makes the bank account look good, but it's not of benefit to anyone. So we think it's important to know that the resources that are invested are invested to benefit everybody in our state.

So the four areas that we thought were appropriate for this investment at this particular time for us had to do with voting equipment, replacement, and upgrades, election auditing, voting registration systems, and management, and addressing cybervulnerabilities in our state.

In the area of voter equipment, replacement, and upgrades, we are currently upgrading all the computer equipment in each one of the 67 counties for five different officials. There are three border registrars that are directly responsible for voter registration, and commissioner, I was delighted to hear you say about the voter registration efforts in our state, which is what we've not been known for in the past, especially under Republican, but we've registered 1 million plus new voters since I've been Secretary of State, and only two words will address that, and that's Roll Tide.

[Laughter.]

The other thing you need to do, we have 3,429,071 registered

voters in Alabama today. Those numbers are unparalleled and unprecedented in the history of the state. But those voter registrars, the three that are there as well as our chief elections official, the probate judge, and our circuit clerk, the absentee election manager, will each receive new computers over the next two years. We started that process on Monday. It will be completed no later that he know September 30, 2019. Hopefully it will happen before that time but we want to make sure that all of those individuals have upgraded equipment that we provide on a state level. Also, it's important for you to know that we are currently working on planning for a more secured election night reporting system where they use dedicated equipment when they're reporting that information to us. We had not had a real-time election night reporting effort in our state in the history of our state. And it's not compulsory now, but everybody participates, and we're excited about that. Post election audits, we evaluate what's best and right for our state. We have paper ballots and retain them for two years. Our voter registration, we want to continue to have upgrades and maintenance. Back in May this year we implemented a two-factor authentication system.

We also ensure our vendors have the necessary security in place to prevent security breaches as we know them today. In the area of cybervulnerabilities, it's important to know that we continue to conduct cyberhygiene scans of our system, working with the public and private partners whenever necessary to ensure that those audits that are conducted and the assessments that are made are performed routinely, so as to ensure the integrity and the credibility of the process.

And we are currently working with as many public and private partners as we can possibly identify. I would share there before I conclude this part of my remarks, is that because of the interesting United States special election that we had in December of 2017, there were a number of things that were introduced in our state that other states had not seen at that particular time related to social media intervention in promoting certain candidates, issues, or policy positions for certain groups.

And we have had the opportunity to interact with officials from Twitter, officials from Facebook, officials from Google in person to help them understand why it's important to make sure that they are also maintaining the effort that's important to ensure that the credibility and the integrate of the entire process on those social media platforms is something that's being checked, vetted, and properly updated. And a number of changes that have occurred in Facebook, placing political advertisements, occurred because of our special US Senate election in December of 2017. So we're very proud of that. We have been excited to work with them as cooperating partners, and I look forward to entertaining some questions that you might have later on in this session. Thank you so much.

>> MEAGAN WOLFE: Well, thanks so much for having me here today. I'm excite to have this opportunity to share information and learn from our other election partners across the country.

So in the state of Wisconsin, we're taking a two-phase approach

to ensuring election security for 2018 and beyond.

The first phase focusing on using the security funds to implement improvements before the November election. Some of the measures that we have taken to improve election security for November include expanding our postelection audit process, and training for our local election officials.

So in Wisconsin, we require audits of randomly selected voting equipment of every general election since 2016. For the 2018 primary, we piloted an additional program, that was aimed at verifying ballot totals.

At the most recent meeting, the state of Wisconsin elections commission moved to increase the number of voting equipment audits for the November 2018 election, and to reimbursement to our local officials that opt into the verification audits. Another immediate need that we identified as part of our first phase was training for our local election officials.

When cybersecurity first became part of elections conversation we would attend local clerk events around the state and talk to them about it. This approach caused their eyes to glaze over in about 15 seconds. They could not see how this new arena of election security applied to them. They were also unclear what the expectations were, and felt like they were being asked to become cyberexperts. So we quickly realized we needed a new approach to training.

In Wisconsin we also have a very unique relationship with our cities, towns, and villages. In most other states, elections are administered at the county level, an average of 50 to 100 local election visuals officials. Each municipality has a clerk.

The Wisconsin elections commission is one of the only agencies in our state with direct contact and shared responsibility with each of these municipalities, and we're acceptable the only one talking to them about cybersecurity. So we saw a gap that needed to be bringing and we filled it with two types of training on elections and cybersecurity.

Reaching our 1,853 clerks at a set time can be a challenge. Two-thirds are part-time and one third of them turn over every year. We want to meet them where they were, and we developed an online learning center, which has hundreds of interactive online video tutorials on a variety of topics and the center allows our clerks to assess the training on their schedule.

The learning center now includes training on cybersecurity. Not just cybersecurity as it relates to elections, but cybersecurity awareness training on topics like avoiding phishing scams, password security, and browsing safely. This year we launched six modules for our clerks. The training was launched as part of our new policy for our statewide voter registration system. Users of our statewide voter registration system must now complete those six training modules and sign a new policy before they're given credentials to access the system.

We developed a table top training program. Wisconsin staff I attended the defending digital democracy event to learn how to run a scenario-based table-top training. The staff at the elections commission -- the Wisconsin elections commission then simplified and

packaged that exercise for the local officials. We trained our county clerk partners to serve as trainers and we're grateful that they were able to serve in that role so that we could have representation around the state. We also quickly realized when we started to enter into this realm of security training that we could not at the time train all the people. So we needed their assistance. These trainings are happening around the state to prepare clerks for the role in any potential security event that may occur.

The second phase of the Wisconsin election security plan involves collecting feedback from our local election partners from the public. With the new HAVA security funds, we wanted to be sure that we were addressing concerns not just at the state level but at the local level too. We have started the process of elect collecting feedback from the election officials on what we need to secure them at the local level. We've solicited feedback directly from the public, asking them what they needed to have confidence in the process.

Our second phase allows us to keep our approach to the security dynamic. The plan we have in place to protect elections today is not the same plan that will be effective in the future.

New information, threats, and resources come to our attention daily.

We need to remain agile and resilient in our approach. There's no finish line. And our approach focuses sustainable resources to address challenges as we head into 2018, 2020, and beyond.

>> KIM WYMAN: I want to put in the official record that we went 2 minutes and 43 before Secretary Merrill said "roll tide."

[Laughter.]

That was a record I am certain --

[Laughter.]

Exactly.

Well, good morning. I'm Kim Wyman and I serve as Secretary of State for the State of Washington. And our state has about 4.2 million registered voters. And we have 39 county auditors who are -- and election officials who are elected and perform the actual duties. Wisconsin makes me feel so much better about that when I hear about those large numbers.

So let me share a little bit about our plan, and how we're implementing the HAVA 2 money. Our state, it came at the perfect time.

We began a project back in 2014 to upgrade our voter registration system, which is a statewide system, over seen by the Secretary of State. The 39 county auditors do upload and all the work and activity to keep the system going and do the data entry on that voter registration system but each county has their own election management system. And all of these systems were purchased by in the early mid-2000s when we went live with our system in 2006.

And like so many states those systems now are old, and so in 2014 we began a process of trying to build a new system.

And my claim to fame is an election official, I got 40 independently elected officials to agree on something.

And we began a process to identify what we wanted the new system

to look like. And this has been a collaborative effort. We worked for about a year and a half, two years to just define the business needs, put it out to the vendors, and we are bringing up the system now, and what it will entail, we call it law vote -- vote law -- it's new. It's a new computer system.

And as we were getting -- gearing up for having it go live in 2019, of course the money was appropriated by Congress. And so for us, it's perfect timing, because we're first trying to build our infrastructure up. The firewalls and things that we have in place. We're beefing up and we're able to do it not only with our current system, gearing up for the 2018 general election, but also having it with parallel Juan eye to our new system we'll be installing next year. The timing was nice to do our infrastructure upgrades. When we started looking at the money well, made a strategic decision to focus one on the partnerships we've been creating since 2016 with our federal partners and state partners, but also to build that cyberunit. I think this is kind of the linchpin for how we will use the money. The partnerships began in 2016 with of course homeland security, the NS, and the ISACS, in our own states with our own IT professionals around the state, our state auditor, and also the National Guard. And what we're trying to do with all of these partnerships is really have kind of a strategic approach to this. First, doing the testing and the assessment of our system, not only at the state but looking at the county systems, and really trying to be very comprehensive in how we approach that -- that security and assessing how our systems are working together.

So we're strengthening those, and what we realized very early on in bring up our new system is that we have a different vulnerability than we had -- than we had with our currently system, in that we're more connected to the counties.

So our system is only secure as the weakest link. That one election worker who works six months a year in a county in eastern Washington, and, you know, is part-time. We have to make sure they are as strong and as well-versed in cyberissues as the person who works in downtown Seattle and King County who is working with this stuff every day.

So what we realized is the counties just don't have the resources that they need to be able to do that. Our 39 counties vary from King County, where Seattle is, over 1 million registered voters, down to counties that have a couple thousand.

And those resources are very disproportionate. So we are going to create a cyberteam, essentially, within our certification and training program who are working directly with our national partners, but also working with the 39 counties to try to level that playing field.

So they're not only going to be doing testing and training of those election officials, like my colleagues, and you've already heard, we've done some table top exercises with them at our annual conferences. And we will provide IT support to those 39 counties.

Again, some counties like King County or Pierce County who have robust staffs, have their own IT teams, but those smaller counties don't and we will try to leverage these dollars to have that higher

level of IT support for them to be able to be aware of not only the cyberthreats but just make sure they're secure. I talked about reinforcing our infrastructure, and another big part of this program is going to be the protecting and monitoring of our systems.

So in our state, like most others, we have our voter registration side and election management side. Those are things that do have interconnectivity to the internet. One of our security models is having the tabulation systems be stand alone, not connected to the internet, and doing the cybersecurity to make sure that flash drives aren't being put in that could be corrupted and there's no way those systems could be connect to the internet. That's the basic outline.

>> JOE ROZELL: Thank you, Commissioner. I'm Joe Rozell from Oakland County, Michigan, the state's second most populous county. We are in a different place than in 2016. In 2017, counties in the state of Michigan began the process of acquiring new voting polling, and Michigan went from a precinct based, paper-optical scan system and upgraded to a digital scanning system. It was a $40 million investment statewide that was focused on improving security. We're also making investments in cyberinformation and physical security as well.

With regard to cybersecurity, we are now in this statewide election security assessment that we're taking part in, as well as for the first time dedicated employees. We have an election security now and within the states of technology management and bulletin, we have a cybersecurity specialist that are available at the state level for both the state and the local level. At the county level we've also spent a lot of time training staff on recognizing cyberthreats.

As well as working with our staff and their social media accounts to remove any reference to them working in the elections department, so that they aren't identified as a threat. Or a target, I should say, by individuals, potential bad actor.

With regard to information, we are doing this comprehensive election security training, as well as postelection audits. So Michigan, for several years now, has been involved in postelection audits. We're now expanding or enhancing those postelection audits to sort of enter the risk-limiting audit arena, and we've begun that process, as well as a complete overhaul of our state's voter registration system. So that originally we had an internally involved voter registration system from the mid-'90s that has not been overhauled and upgraded, and that process is just completed.

At the county level, I would say physical security, we've invested significant dollars in physical security. We recognize that providing individuals with access to voting equipment or tabulation equipment is very problematic. So we've invested in alarms, intrusion detection systems, enhanced video surveillance and monitoring systems of these facilities.

Our tabulation hardware and software resides in a building that is guarded by sheriff's deputies 24 hours a day. We've made investments in physical security to detect and prevent access to this equipment, up to, during, and after the election.

And so we appreciate Congress and the EAC's efforts with these

cybersecurity grants. We're viewing it sort of hopefully as a down payment, if you will, because there's a lot of work that's still ahead of us, and as the secretary from Alabama has mentioned, this is -- this is sort of the new normal, if you will. And so this is something that we will continue to be vigilant about into the future. Thank you.

>> THOMAS HICKS: Thank you all for those great comments and discussion.

I have a few individual questions. Secretary Wyman, I want to start with you. Along with Colorado and Oregon, Washington is one of the three states entirely vote by mail. Does this present any unique challenges or opportunities when it's facing for election security? And do you have any advice, election focused on any state that wants to do entire vote by mail?

>> KIM WYMAN: Yeah. Vote by mail. I forgot to mention that little detail.

[Laughter.]

My state is a vote by mail state, and yes, I think -- I think you're going to see more and more states moving in that direction over time. I can tell you from my perspective when I hear of states who do early voting, absentee voting, poll site voting and have a robust permanent absentee program, you're running four elections at once. And we went through a close governor's race a few years ago, the closest governor race in history. When you do two elections simultaneously, you can't do everything as well as you would like to. And you will see as the cyber issues increase across the country and you will see more states reevaluating the services they provide.

Vote by mail is very convenient for voters. I realize the further east you move across the country it becomes more and more foreign and I know a lot of my colleagues look at me like, "You do what??" But I think from a security standpoint, it helps us to be able to have more controls in place. When I think about our environment before we went to vote by mail where we had thousands of polling places open on election day, we had literally thousands of people who, if we were lucky, we got to train one day a year. If we were lucky, they worked for six days a year. And if we were lucky -- I don't want to say they were young enough to dealing with technology, but the average age of my poll workers when we went to vote was mail was 70.

My biggest points of failure as a county auditor were the people in the polling places because we didn't have the resources to train them and help them be successful. And if you remember back in the 2000s when we moved to the Help America Vote Act and all the requirements that entailed, we added more and more things for those poll workers to do.

Now, as you move of -- you know, all these years later and all of the other things we've added on to those requirements, it really is setting election officials up to fail, because there's so much to do and so much plates to keep in the air on election day or in the voting pardon for that matter. So I think vote by mail's strength is that you have less people who are actually administrating the elections, typically they're more professional because they're

working year-round in that field alone and we have more ability to control those access points that bad actors would have.

So I think -- but it's also a challenge because we don't have as much accessibility on election day that other states do.

>> THOMAS HICKS: Thank you. Director Rozell, you completed a new clause for purchasing voting equipment. Can you tell us what that's like, and some of the new -- some of the additional considerations you used in making this decision?

>> JOE ROZELL: Sure. Michigan replaced a voting system that had been in place since 2008. And I will tell you, it was a significant investment of both, you know, human capital, human resources, as well as financial capital and resources. It was a two-year process. It was part of a state committee that went through drafting functionality requirements and features that are desired, drafting an RFP, receiving and evaluating responses, performing certification testing, working with the EAC, and contract negotiations and implementation. It was a significant undertaking, and I will tell you that when we got to the RFP response phase, you know, we recognized that there was going to be a funding shortfall, that we did not have all of the funds available to cover the acquisition of this new voting system statewide. So we approached our state legislature for an appropriation, and I will tell you that initially our state legislature was very reluctant to appropriate approximately $10 million of funding to shore up the short fall so that the 83 counties in Michigan could acquire this new voting system.

The expense was always one of -- borne by the locals. The legislature was worried about establishing precedent, if they appropriated this money.

But we framed this in such a way that the importance of security and the importance of getting all 83 counties across the finish line at the same time so that we didn't have, you know, a case of sort of the haves and the have-nots, where counties that could forward it would have, you know, a more secure, newer voting system, and counties that couldn't would sort of be left behind. Working with our legislature, they recognized that argument and did appropriate the $10 million so that we were able to get all counties across the finish line at the same time.

Aside from the desire to improve the voter experience, I will say that a big factor in our decision to acquire a new voting system was the increased and improved security that exists now, versus the system that we acquired back in 2004. We were moving away from an election management system that was really developed in the mid-'90s, late '90s to one that's a lot -- a modern platform that was sort of built from the ground up, not code layered on top of code, so that was an important factor for us.

The digital security keys with two-factor authentication, gone are the days of having a metal key that controlled all of the functions. It's a digital key with a password-protected, two-factor authentication. We were able to use complex passwords and assign different roles to different employees, based on their role in the organization or the election works out in the precincts. And the

tabulation computers now have an embedded operating system, and operate really in a kiosk mode, so that's all you can use these for. You turn them on and they go directly in the program. You don't have the ability to install other software. They're not connected to the internet.

So we were very excited to be able to replace our voting system because of these increases in security, improvement in security. EAC certification was mandatory in our state and we work cooperatively with the EAC because all vendors required some modifications to their system. All states are different, do things a little bit differently. And we work cooperatively to get those systems certified at EAC and again at the state level. It was, again, a very involved process, but one that I think was very important to do in advance of this upcoming election.

>> THOMAS HICKS: Great. Thank you. Administrator Wolfe, you mentioned something in your remarks about no finish line, and I believe that's the case across the country, that they are going to be doing this -- that we are going to do this in perpetuity, that whatever threats we have today are not going to be the threats for tomorrow.

And Wisconsin recently issued a notice of recruiting or possibly hiring someone to do election security. A lot of offices are thinking about this and thinking about moving forward with it.

What was your experience like when you did this, and what sort of advice would you give other offices on hiring security professionals?

>> MEAGAN WOLFE: Thanks. One of our first priorities with our phase 1 of our election security plan was to hire dedicated staff that would be dedicated to election security.

And so we recently recruited for and actually onboarded staff in the roles of election security lead, IT project manager, data specialist, security trainer, and a voting equipment certification and postelection audit specialist.

So while we're hiring these dedicated positions now, it does not mean that these important election security roles were not being filled previously. Our entire staff was focused on security. This new focus meant their attention had to be diverted from their traditional tasks to focus on election security and that meantime that things like updating our training and our forms, manuals, and even some IT tasks like creating efficiencies in our systems, those had to be moved to the back burner so that or staff was able to focus on election security.

With this new dedicated security staff, our other staff will be able to turn their attention back to the mechanics of election administration, although the expectation will always remain that they will keep security at the forefront of what we do.

Because existing staff had been filling many of those crucial roles already, we were fortunate to find some internal candidates who had grown into the roles and developed skills that were very specific to election security.

As the field of election security has grown, our staff has pursued professional development and fine-tuned a unique skill set

that in a lot of ways were able to meet our needs in a way that would otherwise be very difficult to hire for.

Internally hiring staff in these special roles allowed us to back fill positions that utilized a more broad skill set, and I think that was something that was surprising me to me but ended up being helpful. And we hired new staff that had experience as election officials. Having staff with experience at the local level and bringing that perspective has been invaluable to us. Especially in roles such as training, like I talked about, training has been a big initiative for us.

And having people that are resonant with that audience and understand the challenges they face has been something that's been very, very effective for us as well.

Based on our experience with hiring, I have a couple of takeaways. Recruiting and onboarding is a lot of work.

And then when new folks come on board there's a lot of time that's needed for that transition as you train them.

This takes up a lot of time. But prioritize it. It's important.

Our jobs as election administrators have grown significantly in the last few years, and there's no way to get everything done unless you push things to the back burner without bring on additional talent. So even though it's a lot of work, I recommend that you focus on that and priorities it.

Another takeaway was invest in your team. Invest in the people that you have. Give your team the resources that they need to be successful.

Sometimes that may mean reorganize -- or recognizing the skills that may be you already have on board, and offering them opportunities for enhancement.

Elections administration and election security changes every day. So other times, it also means allowing a team member to grow and evolve into a new role, to meet a new need. Then back filling that position that might be a little easier to recruitment for with more traditional skill sets.

>> THOMAS HICKS: Thank you. Secretary Merrill, you were recently in the news talking about steps your state did to secure elections.

Can you talk a little bit more about your efforts to register new voters and the HAVA narrative that you've done with this?

>> JOHN MERRILL: Absolutely, Commissioner, and I appreciate the question.

I think that it's so very important to realize that because of where we are today, we have to continue to concentrate on training. When you look at the military, law enforcement, our firefighters, they spend the majority of the time that they have each and every day in preparation, in understanding for the event that may occur at some point in the future.

And that's what we have to do, and that's what we're doing in Alabama.

One of the things I was very disappointed in when I became the secretary -- actually, before I was even inaugurated, I went to a

program in Colorado -- I'm sorry -- in California, and I met Wayne Williams, and he introduced to me about the outstanding election training facility that was located at Auburn University in Alabama!

And I asked him a few more questions. And the thing that was disappointing to me was not that it was at Auburn, which is what most of y'all might think --

[Laughter.]

But I don't know anything about it. Because it had never been introduced to me! And we haven't talked about it in the legislature. We didn't talk about it with our election preparation. It was just not something that was introduced. I found out that very few of our people ever went to Auburn for the training! People were coming from all over the nation to take advantage of that training! And don't get me wrong, now, because y'all know I love Alabama. We've already talked about that.

And Auburn is an outstanding place to live and an institution of higher learning, one of the finest of the nags if they didn't have an athletic program.

[Laughter.]

But what's important for you to know is that the quality of the work they did there in preparing people for elections is unsurpassed in the nation. And so we started a program of training for our board of registrars, which are our local election voter registration officials who are required to go and attend a program. We contracted with Auburn over a three-year program to ensure everybody had the training to be prepared, because you can never train enough. And when you think you've reached the point of saturation, that's when the event occurs, and that's when you are caught in a bad way. And we don't ever want that to happen.

Thomas put one on the tee for me when he talked about voter registration. Because the commit that I made when I became the secretary was to ensure that each of every eligible US citizen that's a resident of Alabama is registered to vote and has a photo ID. We passed the voter ID law in 2011, 2014, I've already talked to you, gave you the numbers on people that we have registered, total number of registrants, and I think it's important for you to know that our commitment in making sure that the ID requirement is being met, not only do we visit all 67 counties every year with our individual mobile units that go all over the state, and I do that too. As a matter of fact, as of today, I've been to 52 of our 67 counties since January 1st, 395 unique visits to those 52 counties that I've been to.

But we will actually go to people's homes to give them IDs, if it's required. I mean, we introduced a mobile app. We introduced electronic registration. We want to make sure that everybody has the ability to participate at the level that they want to participate, so they can be a part of the process.

Thank you, Commissioner.

>> THOMAS HICKS: Thank you. Thank you. Is there another school in Alabama that we haven't heard of?

[Laughter.]

>> JOHN MERRILL: We have several institutions of higher

learning but if you want to talk about practice again, you can see what the results are when you look on the football field on a Saturday. That's why it's important to be prepared!

>> THOMAS HICKS: [Laughs.]

>> JOHN MERRILL: Even if it's second and 26.

>> THOMAS HICKS: We will open it up for questions from the audience. And again, we ask three things: Speak into the microphone. Natalie has the microphone. The microphone is up here. Speak into the microphone so people can hear you. Raise your hand. And give your name, affiliation, and most importantly ...

There you go. Ask a question.

All right? Eric Fisher?

>> AUDIENCE MEMBER: Good morning, Eric Fisher, Congressional Research Services, the Library of Congress. I was wondering, there was some mention of audits, and that's become a big thing among the security folks, and I was wondering whether you all have considered that or had experience, what -- what are you finding and what are the benefits and disadvantages, how you think it should be implemented.

>> JOHN MERRILL: Well, I think -- I may be the only one on the panel that's not already fully engaged in this effort, and that's one of the things that I was disappointed in, is that we did not have an effort already in place. Because I don't think, if you -- if you choose not to accurately measure what's already occurring and validate it by checking it and doing spot checks or things that are necessary to figure out if things are actually the way they appear to be, then you're just setting yourself up for exposure at some point in the future which is negative, and then you've got to respond to the questions about why this was not being done before.

So you have to have a way to properly audit and make sure that you're checking against it feels that look as though they are standards already.

And so that's what we've been doing, evaluating what other states are currently doing to see what's right and best for Alabama.

>> MEAGAN WOLFE: I think another important thing is there are different types of postelection audit. A risk limiting audit is a very specific type of postelection audit. In the state of Wisconsin, because we have a vast diversity of voting equipment and municipalities, risk-limiting audits is something that requires everybody to be on the same type of voting equipment or to have more consistency as far as what that process looks like. There are other post-election audits, and the goal is to ensure that the votes have been tabulated correctly.

And we have equipment audits after general elections, and that's for the purpose of making sure that the voting equipment is tabulating the votes correctly. So there's a lot of different types and we've been exploring how those various types could be used in a system like ours.

>> KIM WYMAN: In Washington State, I mentioned I totally overlooked the obvious one, the springs of vote by mail. We're a paper ballot state. And our state, we've done pre- and postelection audits. Obviously, the accuracy test and those type of things.

We do have legislation that is enacted this year that will bring

the opportunity for counties to do that, but for similar reasons you've already heard, we're not doing them just yet. But we do -- we do actually audit a random office that's picked by the two political parties after the polls have closed, and -- or excuse me -- after the voting period ends, and some things die hard -- and then there's an audit there, and then we also have manual recounts that are triggered by less than one half of percent or less than one-quarter percent. So we already have those in place. We're working towards risk-limiting audits. We're looking to Colorado's model and some of the things they've done there but it's a challenge because we have different voting systems and now all of them lend themselves well to finding the ballots easily. So we're working through it.

>> JOE ROZELL: And we know that everything is great going in, and I think it's an important process to including afterwards to make sure that we can have confidence in the results. It takes time. It takes resources. But I think it's necessary, these audits,ing a part of the process. And they've not yielded anything in our state that has shown anything significance with any of the voting equipment. All of the audits have shown that the devices are recording correctly.

>> THOMAS HICKS: Any other questions?

Wow, I'm surprised.

>> AUDIENCE MEMBER: Good morning. I want to riff on something that Meghan said on hiring in Wisconsin. I'm curious if the panel thinks that the future of personnel are going to be promoted from within? Use people who know and teach them cybersecurity or has there been any thought on recruiting folks who are interested in cybersecurity and bringing them into elections? Thinking about the future of the election cybersecurity workforce.

>> THOMAS HICKS: I wanted to get on to this. I know I'm the moderator, but moderator privilege. I get the distinct honor of being able to travel around this country and seeing a lot of institutions and seeing a lot of election officials.

Last week, I was in the state of Florida, and was speaking down at the -- or it was national voter registration day on September 25th, and we went down to Pensacola State College, where they have a great cybersecurity program, two-year degree, and those folks come out of there ready to be hired and put into the workforce to help out with the threats we're facing today. I'm sure there's other schools around the country that are also doing it. But they put out, I think, at least two or three hundred folks every one or two years or so. Or I might get shows numbers wrong. But they have a great program down there as well. But moderator privilege fasts off.

>> MEAGAN WOLFE: I think one of the other challenges in hiring for election security, we work for state governments. And it's hard to match the rates in the private sector.

And so we -- you know, we were very successful in being able to grow our staff into those roles.

We had staff members that may be had some technical skills and knew a lot about elections and we were able to combine those two things to continue to get them more education. For example, one of our staff members, we were able to get him through the process for

becoming what they call a white-hat hacker, so we could do penetration testing. And we found that investing in our team and staff, growing the skills that you already have was a successful way to sort of fill those needs in what would otherwise be a very challenging market to recruit for.

>> KIM WYMAN: When your home state is Microsoft and Amazon, you talk about tough to compete with it. It definitely is.

We have had a pretty robust IT team in my office for many years, and have worked with Washington National Guard and continuity of operations planning, so it dovetails nicely that we're working with them on the cyber side. And we have this great resource because of Microsoft and Google and Amazon being -- having such a presence in Washington that a lot of the guard members, that's their day job and when they serve in the Guard they help us build this robust team, and Doug, you're right. The challenges, do you teach election officials to be IT professionals or the other way around and I think it's a mix of both. That's why creating this position and adding five IT specialists that will bring the technology background to our elections.

>> JOE ROZELL: Our chief security officer for the county is our actually highest-paid county employee. He pass the medical examiner, it was a medical doctor. Despite that, they are the highest-paid county employee. It's difficult to keep them when you're competing with our private sector. We're on our second chief security officer. This one came to us from the banking industry.

So we have found that bringing folks in from the private sector and brings them up to speed on elections has worked well, but recruitment and retaining these folks, I believe will continue to be an issue going forward.

>> JOHN MERRILL: And we do have to have the intention although of hiring professionals that are dedicated for this purposes and we have to make sure our team members on board stand it's incumbent on them to continue to invest in educational opportunities to learn more about what they need to do to be responsible in this effort and how they can contribute, and their jobs, and be cross-trained to understand when positive spite things and what do to do to be a more effective team over all. Thank you, Commissioner.

>> THOMAS HICKS: Before we go any further, I wanted to acknowledge Garrison from the Senate rules committee. Without his help, we would not be in here today. So, you know, with all the ...

[Applause.] [Speaking away from microphone].

[Laughter.]

[Inaudible].

[Applause.]

>> THOMAS HICKS: So I've been told that we have about one -- time for one more question.

So who has the microphone? I guess they have it in the back there.

>> AUDIENCE MEMBER: I'm Colleen Long from the Associated Press. I wondered if you guys could talk a little bit about the collaboration between the federal government and your states on election security. Has it improved? How is it better? How is it

not better? What needs improvement? That sort of thing.

>> THOMAS HICKS: Again with moderator privilege. The EAC is offering to states IT training for election officials. And it's offered free.

Our testing and certification folks go down to state conferences and train folks, either three-hour or six-hour course, letting them know what to be prepared for, some things they should look out for as well.

And as we've come to the closeness of our 2018 election, I think that we have one training class left, but I think come January we're going to be offering that up for other states as we move forward.

I think that another piece of the partnership that's been working really well and that we've improved upon for 2018 as opposed to 2016 is the critical infrastructure piece, of making sure that we get that information out to the states quickly and accurately, so that they know what they should be looking out for. With the Albert monitors and other pieces that we've -- that have been implemented by our federal partners.

And with that, I'll quiet down because it's not about me. It's about the people on the panel.

>> JOHN MERRILL: Commissioner, we want to continue to work with the public and private partners. It's important for everybody in the room and all the people within the sound of our voice to remember that with our private partners, if they are not committed to excellence in this area, they won't be private partners very long because they won't have a relationship with us and they won't be able to get business from other entities. But our public partners, especially homeland security, the National Guard, the EAC, all of the groups that you can think of that may be trying to help us and support us are welcome to work our state. We have found them very, very accommodating, very interested in working with us and trying to ep had us be the best that we can possibly be.

The one reluctant that we have in the state, this may be something that's been introduced to some of y'all for the first time, but in Alabama, we don't like being told what to do. And whenever somebody appears as though they're trying to initiate what needs to happen and the why and the way it needs to happen, that's not often received with open arms. Whenever you intimate that you'd like to be a part of a team to help us be better than we currently are or introduce new thought processes or ideas that we can receive and that we can implement so we can be better, we're for it. And we want to work with you. And that's what we found our public partners to be doing so far.

>> KIM WYMAN: I will be the first to admit when the critical infrastructure designation came down and some of the initial contacts we were having with the federal government, I was skeptical. And I was probably one of the harshest critics of the idea of the federal government coming in and taking over our elections. I still am. But I can tell you that in the beginning it felt like an arranged marriage. I think that's probably the best description. Particularly our partnership with homeland security. But what I can say is that the leadership at the top set the tone. Secretary

Nielsen has done an outstanding job of listening to officials across the country from Secretaries of State all of way down.

And those partnerships are really positive now. I think we're in a very different place than we were even at the beginning of this year. At least speaking for my state.

And we are getting access to resources that we couldn't have had a couple of years ago as a result, and so we had some of the things to work through, and I think most of them were communication channels, to describe honest. I'll give you an example in my state, that the MSIAC would contact our OCIO and have meetings and talk a lot about my system and never call my staff or me, and that was problematic, and it was -- it was difficult to express, because of course, I would have to talk in terms of silos, which I don't like to. The governor staff reports to the governor, and my staff reports to me, and I'm responsible for the election and you have to stay in the lane and now they get it and I think the partnerships are yielding a lot of really positive things.

>> THOMAS HICKS: With that, I think that we are going to wrap this up, and I'm going to go to introduce the Senator, I believe he's on his way in. Or should we do one more question, maybe? One more question. I think Susan had a question. I saw her hand first. And, no, these are not plants. This is me recognizing people. So ...

Wink-wink. [Laughs.]

>> AUDIENCE MEMBER: Thank you very much. Susan Green, policy director for national election defense coalition. And I want to commend everybody for the information that they're sharing and it's really impressive, how much the election community stepped up to improve the security and it's evident from all the information provided by this panel. I will get to my question.

And the one thing that I find that there is an absence of attention to is the question of internet voting, which is a concern for 32 states that use it in this country. It's a vulnerability to our system. And we don't see it addressed. When France had concerns, they cancelled their internet voting.

I'm wondering if there's going to be any attention put on that issue from the federal level. So that's to you, Chair.

>> THOMAS HICKS: From the federal level, the states run the elections. So ... [Laughs.]

So -- so we are not getting into I guess internet voting for our own -- dictating to the states so what they should be doing. I think there are states out there that want to open up the -- allow for those who have access to their ballots in terms of if they're fighting in Afghanistan or Iraq, and they -- or even for countries that don't have good mail systems, so make sure that those folks still have access to the ballot.

And so opening it up to various ways, I don't know what sorts of things that these states are doing in terms of electronic ballot. But in terms of security, it would be to allow to make sure that no matter what method that states are using, to return the ballot, whether or not that's mail or being at the polls or electronically, to make sure that the safe guards are put in place to allow for those to be done securely and accurately.

With that, I think we're going to wrap up this panel, and I want to thank each and every one of you for taking the time. I know it's a very busy season for you to break away and be here.

And so I want to thank you all for being here, and I will step to the podium -- thank you, and go to the podium and start to introduce the Senator.

[Applause.].

So we are -- here we go.

We are very honored to have, you know -- I want to thank the panel again. That was a terrific discussion. And a perfect prelude to our next speaker. We are honored to be joined by Senator Roy Blunt from the state of Missouri who was generous enough to sponsor this space. As a public servant, University president, teacher, and United States Senator, Roy Blunt was elected to the United States Senate in 2010. Senator Blunt serves as chairman of the Senate rules committee, and administration committee, and vice chairman of the Senate Republican conference. He also served on Senate appropriations, Senate commerce, science, and transportation. Elect committee on intelligence, and in addition accesses as chairman of the appropriations subcommittee on labor, health, and human services, education agencies. And the commerce secretary -- subcommittee on aviation, operation, safety and security.

The people of southwest Missouri overwhelmingly elected Senator Blunt seven times, the United States House of Representatives. Senator Blunt was elected majority whip earlier in his career than any member of Congress in over eight decades.

He was elected to Senate leadership during his first year in the Senate. During Vice Chair McCormick -- please. Please.

[Laughter.]

I hate these things. Thank you.

>> ROY BLUNT: Thank you all.

[Applause.]

Glad to be here. I should have stopped earlier. But I was enjoying it there for a while, and I thought we'd just gone a little bit to far. I'm glad you're here. I appreciate what you do. I have served on the intel committee and it's been a big issue for us the last year and a half. I serve on the rules committee, which is the election verification committee, and beyond that, you know, for the first eight years I was -- the first 12 years I was a public official, I was the local election authority in the biggest county where an elected person did that job, as opposed to a commissioner, a board of election commissioners in our state.

The eight years after, that I was the Secretary of State, the chief election official for my Secretary of State friends who are here, I'm still a dues-paying member of NASS, and it was one of the best organizations I was ever a part of, both for myself and my family and we enjoyed it greatly.

But speaking to an event a couple of weeks ago in St. Louis, the Secretary Ashcroft hosted, eight or nine Secretaries of State there, and a number of Missouri officials but more from around the count. It occurs to me as I was giving the speech, of all the public responsibilities I had, I don't think I took any more seriously or

felt more my reputation, my responsibility on the line than when I was either the chief state election official or a local election authority.

They know exactly where to come if something goes wrong on election day, and Murphy's law, if it ever applied, it applies on election day. But I think that's one of the reasons I'm so committed, as I believe my colleagues are, to continually have the fundamental responsibility for election administration to be at the state and local level. I think the federal government can do some things to help.

And I also believe that in this year's election, everything that Senator Klobuchar and I would like to see happen by statute is basically happening.

Now, from my point of view, I'd still would like to see that memorialized in law so that five years from now or six years from now or 10 years from now, it's still continuing to happen, that the federal opportunities and agencies and backup that's available to you is available in a way that we all are clearly understanding and comfortable with.

We are not going to get anything in law between now and election day, which probably makes it even more important that we immediately look back at this election and say, okay, what happened that should have happened? What happened that shouldn't have happened? What kind of deference was given people who have been elected to do these jobs? What kind of security and clearance and immediate access to information was given to people who do these job?

And I can guarantee you that I'll be very committed to doing that. I think our committee will be committed to doing that, and on we're going to continue to work that direction. The FBI director about three weeks go now said that people should have great assurance that everything is being done to secure the election system itself. And I think that's accurate.

I think we're all at a heightened level of awareness, hopefully at a heightened level of information sharing. And we're going to continue watch closely and communicate both with the election assistance commission and homeland security to see that those things are happening. We don't want a situation again where a few weeks before the election suddenly state officials are told "We've decided we will declare this a critical infrastructure."

The last thing you want is a big surprise at the last minute. Auditing, clearly many states are doing everything that I would hope we would see in auditing. That was a big concern to many of the state election officials that contacted us, when we thought we had a bill that everybody agreed on. The auditing and how that would happen -- that would happen became a problem.

I personal think that there should be a paper trail, something that can be counted after the election. I also believe that that's where everybody is headed, whether they're there right now or not. And I think the greatest assurance you can give voters about what happened on election day is not only do we go back and spot-check and verify that what we announced happened is what happened, but we would have the capacity in any election at any time to go back and actually

have something that voters held in their hand, looked at, saw what they were trying to do and that's been saved just like paper ballots, before voting machines were saved.

So we're -- we want to work with you to this.

The central thread of the fabric of democracy is people having confidence that what we were told happened on election day is what absolutely happened.

Sometimes it's hard enough to accept the results of an election, even if you are fully convinced that's what voters wanted to do. It's certainly hard to accept the results of an election if somehow you think there's any question about that. So as we do more verification, as we try to create more certainty and assurance in this process, we will work with you to do that. Senator Klobuchar and I are both committed to that. I'm glad to get a chance to work with her on the rules committee that we work on together. And look forward to both of us continuing to work with you. Thanks for letting me come by for a few moments today.

[Applause.]

>> THOMAS HICKS: Thank you again, Senator Blunt. And I attended that event in Missouri, and was very pleased with Secretary Ashcroft in putting that on. It was helpful, and I think those who were in attendance really learned a lot.

Once again, I want to express my deep appreciation to both the Senators here today and introduce our next speaker, Senator Amy Klobuchar who serves as chair of the Senate Democratic steering committee. Since arriving in 2006, she's worked with Republicans and Democrats to get things done, including landmark legislation to end human trafficking and the opioid epidemic. She's fought to protect consumer protection and more than a generation, and has pushed the cell phone industry to enact more consumer-friendly policies. And with that, I introduce Senator Amy Klobuchar.

[Applause.]

>> AMY KLOBUCHAR: Thanks for your work. Thank you. It's great to be here with Senator Blunt. There's a few things going on in the building this week, but we're focused right now on some work that we have been doing together for quite a while, and in fact, Roy and I cochair the adoption caucus, and the tourism caucus, and then my favorite thing we did this year as leading the rules committee is that we got Tammy Duckworth came to us after having the baby, and she's in a wheelchair with no legs because of her service in Iraq, and she asked if she could bring the baby on the floor, so Roy and I had to work through a rule that had not been changed in hundreds of years, except to allow a dog on the floor in the '80s, and we were able to get this through a lot of senior members. My favorite comment, one of the Senators said to the press, maybe we could have this baby on the floor, but what if we have 10 babies on the floor!

And I said, we already have 10 babies on the floor!

[Laughter.]

So there was this amazing moment where Tammy wheeled herself on the floor with this little 10-week-old, six-pound baby, who slept through the entire historic moment. It was just a lot of good work we do together as part of it. I want to thanks, as well, the

chairman, Vice Chairman Christy McCormick and the staff, thank you, Secretary Jim Condos. We've had some interesting discussions recently about the secure elections act, and he's standing up for all of the Secretaries of State concrete country and we hope we can work this out. And I want to thank you for all the work you're doing on the front line. I had a job similar to this. I was the county attorney in our biggest county, and I knew what it was like to have these mandates come from the state or the federal government. And oftentimes, they would send something down and there would be no money, and we'd be stuck being the ones having to do it, and we don't want that to happen here, and I think that is why we actually started out this year as you know with that $380 million that Senator Langford and I and others on the appropriations committee and Senator Blunt all supported, and I know most of that money has gone out to the states, and it's in various stages, but we thought that was very important to do.

At the same point because we are really dealing with a international threat, and it's not easy for a state, whether Arkansas or Maine or North Dakota to deal with that by themselves and that's why we are also looking at some of our rules and laws and how we can make sure using the expertise from homeland security and that we have here that we use that expertise and make sure if we're going to give money in the future, we at least have -- I would say, I want to say in the nicest way -- a carrot and not a stick tied to that funding, which is why we would like to get this bill passed. And that would include, as Roy mentioned, the backup paper ballots and we're looking at doing possibility pilots with audits, and of course making sure that homeland security is giving the information, okay, that was homeland security, I know.

[Laughter.]

Was giving the information. Lindsey, our chief council! Thank you!

[Laughter.]

But giving the information, as soon as possible, to the states. As you know, that was a problem when 21 hit states we found out were hacked, including my own, the state of Minnesota, and didn't know there were attempts to hack, including what we found in the indictment out of the Justice Department of the GRU members, the Russian intelligence people who violated our laws, and it doesn't say which state, we have a suspicion, but actually accessed data of 500,000 voters. Those are real things happening right now, and I kind of have an adverse reaction when people call it "meddling" in our election. That's what I do when I call my daughter on a Saturday night and ask her what she's doing. Okay? That's what that is.

But to me, this is much more of an organized cyberattack, and while the focus has been on Russia, because of 2016, it could easily be another country or another criminal organization, and we have to take this seriously. And that's why I think part of this is stepping back a little and thinking, how we always do things, how we always did things this way, we're going to have to do things differently. I love that we have a decentralized election system. I think that's one of our protections, that we don't have everything the same in

every single state. But at the same time, what Senator Langford and I did with the bill is saying, okay, what are some things we can do, working in that structure to make sure everyone gets the message that we want to give you more money to states to help you, but we want to make sure that we take those best practices that we know are working, which is these backup paper ballots or we know will protect us if there's a hack. Because part of this, while it is the individual state interest, it's going to affect the whole nation. If one county in one state or if one state gets hacked into. So that's the perspective we have in addition to the work that we're doing with the states.

We are now 31 days away from the next election. Who's counting?

And you look at what we have learned from past elections, 2000 election showed us the shortcomings of the butterfly ballot. Bring that up.

And 2016, of course, we learned some of our own shortcomings with what we saw. Another thing that isn't really in the election hardware-software space but about the propaganda issue when doesn't exactly affect firsthand election officials in your day-to-day work, but another concern that we have in that the security people had under both President Obama and President Trump is just what we're seeing on social media. And I just put that, since you guys are experts in elections, something that I know you'll hear about and should think about. Senator McCain, and we miss him every day here, and I and Senator Warner had a bill, and it's still in there. We're trying to get a Republican as a lead to take Senator McCain's place on the bill. But it says that the major platforms should have to put up ads for disclosure and disclaimer, so you're able to see who's paying for them and what they are, both for issue ads and for candidate ads, and it exactly mimics what we do for TV, radio, and newspaper.

Because as you know, 1.4 billion was spent -- 1.4 billion -- or internet ads for the political campaigns in 2016, and the forecasts for 2020 is like three to four billion.

Now, fortunately, because there was a little hearing about something called Cambridge Analytica, and Mark Zuckerberg had to testify. We want to have the same rules apply across the board. And that's why we're trying to pass the bill. And I hope when we get out of the election time period, we will be able to get this done.

So when I would like to see as we move forward, as first of all, more information sharing, and we know that homeland security is now working and have made this a high priority.

I'd like to see our bills passed. My bill's passed, the one is helpful, we have a new version coming out and we ask you to work with us. I would love to have is get passed in the lame duck, for people that want to delay it or stall it beyond that, well, that's up to you. Because then we'll have a new Congress. And I think it would be better it to get it done as soon as possible, and we are certainly ready to go with that.

And we simply have to call the markup, which the chairman can do, because we've already had a hearing on it, and then it could go to the floor. We have a similar bill in the House. And I think that

would be good if we could possibly get it done by the end of the year, working with the administration.

And then the last thing is I think we will need more resources, going forward.

And I think getting the bill passed would be really helpful as a precursor to then getting more resources that you need as we go into the 2020 election. Obviously 2018 is going to inform us as we go into the 2020 election.

So mostly, I want to thank you for your work. I would be remiss not to mention that Minnesota had the highest voter turnout in the last election!

Yes!

And a lot of that has to do, I think it's like three-fourths of our eligible not voters but citizens actually vote. It's an incredible thing. And a lot of had has to do that we have same-day registration, and then we also just like many of your states, of course, have been using early voting more, but it's not the only way, because we also have the same-day registration.

And I've seen that the states that move to that, whether they are more red states, like Iowa or some of the other states that are more purple states, tend to have higher voter turnout.

And I hope we can keep working with you on those kinds of measures to increase voter turnout because it's important. And the other side of this, I know because I used to be the county attorney for eight years, and we got the election cases that would come in our door all the time, and we brought a few cases against people that had double-voted, and I'll end with one moving election story.

We once had a couple that double-voted because there was a school board race and they double-voted because they decided -- the school board line ran through their house. And they decided that that would be fair then, that they would vote in both areas.

And they unfortunately also voted for the state races twice. Right?

It comes to our attention, and they call our prosecutor and said, where are we supposed to vote? After we resolved the thing.

And we looked at it, and we called them back and said, "Well, in the future --" I think they were banned from voting -- "you have to vote where you sleep."

And the next day the woman called back and said, "What if we slept in separate rooms?" And we said, we don't want to get -- that's called TMI, and we do not want to know that.

[Laughter.]

I am aware of all the hard issues you deal with every single day and I want to thank you very much for your work. Thank you.

[Applause.]

>> THOMAS HICKS: I want to thank both Senators for taking time out of are their busy day to be a part of this.

With that, one piece of caveat is that those born in the year 2000 when most of this started happening are now eligible to vote in 2018. So they're now 18 years old. And with, that I'm going to turn this over to vice chair Christy McCormick for her panel.

>> Ladies and gentlemen, our program is about to begin. To

start again, we'll have a break after this session.

>> Thank you so much. We're going to start our second panel just a moment. Thank you.

>> CHRISTY McCORMICK: I want to thank Chairman Hicks, and on behalf of the EAC, I thank Senators Blunt and Klobuchar for their remarks. I'm pleased to join you for this next set of panels. I'm Christy McCormick and I've got a great panel.

Election officials are always striving to improve the voter experience. While their constant internal planning often goes unnoticed, those of us who work in elections know the importance of these efforts. We're thankful that election officials are always thinking about the process or procedure that they can retain, a system that needs to be remediated or replaced or a potential crisis that might require a contingency plan. We're thankful for this, because it's these efforts that ensure that Americans have access to the very elections that serve as the bedrock of our republic and our democracy. Our discussion will center around how best to serve voters during the 2018 federal elections and beyond.

Joining me are from my far right, Secretary of State of West Virginia, Mac Warner, the 30th Secretary of State of West Virginia. He's been the defense attorney and a chief prosecutor. He rose to the rank of lieutenant colonel before his retirement after 23 years in the United States Army. Thank you for your service.

After retirement he was called upon to run the organizational capacity building section of the world's largest rule of law program in Afghanistan for the US Department of State. For five years he mentored Afghan Supreme Court, the ministry of justice and the ministry of women's affairs. He spent his life promoting the ideas of freedom and democracy around the world. He understands a vibrant free market economy only occurs when clean fair elections have provided a safe environment where investment can flourish.

Next to me is Paul Lux who came to Okaloosa County in Florida. He was elected a supervisor of election in 2008. He currently serves as president of the Florida state association of supervisors of elections. Paul has kept Okaloosa county on the leading edge, participating in beta assessing and certification testing, equipment upgrades.

He has been deeply involved in improving voting for absentee military and overseas voters. He has participated in the voting over the internet project, the secure electronic voting and registration experiment, the Okaloosa ballot delivery project, a lot of innovation experience. Thank you for joining us today.

On my left is Sherry Poland, the director of elections at Hamilton County, Ohio, the third largest county in the state. Responsible for the day-to-day operations and administration of all local, state, and federal elections. Hamilton County was among the first counties in Ohio to implement electronic poll books, automate the election day and create a youth at the booth challenge for high school seniors to work at the polls.

She served as the board's operations administrator, responsible for all aspects of the vote counting process.

Welcome, Sherry. I look forward to the discussion.

And on my far left, not that he's on my far left, but --

[Laughter.]

I owe you an apology, Secretary Williams --

>> Do I have to say Roll Tide?

>> CHRISTY McCORMICK: There is a error that said Secretary Merrill. Secretary of State Wayne Williams is the first Colorado Secretary of State to earn the national certificate election administrator.

Prior to his election as secretary, Williams served as the El Paso county clerk and recorder from 2011 to 2015 where he successfully ran elections in the states most populous county. As clerk, Secretary Williams focused his efforts on expanding services to citizens by adding more than a dozen 24/7 drop boxes and consistently running elections cost effective and voter friendly, expanded access to online records.

Secretary Williams received the medallion award for his effort to protect the right to vote in 2012.

For serving as county clerk, citizens of El Paso County elected him as commissioner from 2003 to 2011 where he helped run Colorado's lowest cost for citizen government while addressing critical infrastructure needs. Thank you for something here.

So I just wanted to say, this panel will focus on the ways that each of you is serving the needs of your voters, and working to administrate secure, accessible, and efficient elections. I want to ask each of you when a specific initiative that we hope to highlight today and then we can dive into other programs and issues. And I'll start with secretary Warner. West Virginia has unveiled some innovative approaches to serving the HAVA voters this here, including a pilot problem that's a mobile app for military voters. Can you please tell us a little bit about that initiative, why you felt it was important, challenges you faced and what's the response has been from the voters who may benefit from this initiatives.

>> WAYNE WILLIAMS: It's an honor to be here, and it's important, thank you to the EAC commission to host an event like this. It's very important for us to all get the word out to the citizens of America, what has been going on, and it's quite different than perhaps the message that has been out there in the press quite a bit. That nobody cares, nobody's doing enough, Congress isn't doing enough and so forth.

My perspective being a little bit on the inside, I've been seeing an awful a lot of work going on and it's quite a bit different. But by way of getting into the topic, when I came in this morning, Leslie gave me grief how I was dressed, how we look like our parents.

And so it reminded me, I'm a new Secretary of State, just like 18 months ago or whatever, and I made it a point to get around to as many Secretaries of State as I could prior to taking office to pick up pointers from them. And I'm in Montgomery with John Merrill and he takes me to his favorite bar, and we're sigh sipping diet Cokes, and across the bar there are two rough-looking characters. And "Hey, John, that's us in 10 years."

And he says, "That's us, dummy. That's a mirror."

A lot of times you look at something and you either see what you want to see or you choose not to see what's in front of your eyes. And that's what's going on with this mobile voting device in West Virginia.

I want you to stick with me here. This a specific solution to an identified problem. To address that, you have to look at risk and reward. And when you hear what I have to say this morning, I would hope you come down on the side that we do, that the reward far outweighs the risk that's going on here.

And so to identify that risk, share with you just a couple of war stories.

My wife and I have raised four children, all of whom served in the military. I did a military career. My wife -- all over the world, and we had difficulty voting throughout that time. And it wasn't because we didn't want to. It was because it was difficult to go through the process, to get through those obstacles. Each of my children have had trouble voting.

My oldest, Stephen, served a year in Afghanistan, and to give you a little bit of a context, he was wounded there, and 13 of his 30 men were rounded in their year in Afghanistan. That starts to give you a feel for these guys who aren't back in the rear. They were on point. They are route clearance personnel. And you way you clear mines, you take a pickax and drag it on the ground and when it catches a piece of wire, everyone freezes, and that's how you pick up mines in Afghanistan. Not a great job. Especially in the heat and with Taliban and snipers and people gunning for you.

And he went through a number of harrowing experiences, and I asked him what his toughest time it was, and he said "Dad, it was election day."

Why is that? And he went into quite a bit of detail. But he was required to secure one polling place, and in the process of the heat of the day, long days, they dug up five IEDs. Okay? Five. So think of the amount of effort that the Taliban was going through, and the risk that American soldiers were put their lives on to go and secure that polling place to secure people to be able to vote in the first election in Afghanistan's history, democracy at work in a foreign land that the soldiers are putting their lives on the line to protect.

Keep that image in your mind. And multiply it times soldiers in 120 countries through the world today on a daily basis. The state department, and people putting in their years of service, in 170 countries around the world. They have as much right to vote as we do, and we owe it to them to give them the opportunity.

In the federal voters assistance program, when they report to Congress after each election, let me give you an example. I'll simplify it so we didn't get into the big numbers. Take a representative sample of 100 active duty military, only 66 will be registered. Only 22 will request a ballot. Only 18 about receive that ballot. Only 14 will return that ballot. And only 13 will have their vote counted. 13 out of 100 people active duty service military will get their votes counted. In West Virginia it was 9 in the last elections. That's the identified problem. And it doesn't

get better on the civilian side. When you get to the civilian side, report dated September of 2018, okay? 2018 route here. When you get into overall citizens serving overseas, it's less than 7. Less than 7 people serving overseas, 3 million people serving in 170 countries, overseas, and less than 7 in a hundred get their votes counted. I see puzzled looks. That's what I had on my face too. I had the experience first hand and so did my children, and I said, we got to do better.

When you get sent into harm's way, you want a voice in who sends you there. You want to vote for the person who will get you out of harm's way.

And I gave that to my elections director, here in the third row and said, we got to do better and solve it to it's transparent. You can do it without electricity because a lot of times you're serves in something that you don't have something to plug into the wall. You got to do it without computers and scanners and printers.

I said, we got to do better than this. And he went to work and found a partner. Okay? Bradley Tusk, the brains and financing behind Uber.

And think how they revolutionized transportation in America. When you start talking about numbers of 7 out of 100 or 13 out of 100, we don't need to be tinkering at the edges or put money towards more videos and programs and federal assistance programs, people out there in the world -- we need to revolutionize the approach we take to getting people the right to vote.

And so that's what we've -- he looked up with Uber. What I love about this technology is not -- it's bipartisan. It doesn't take sides.

So here I am. I'm a Republican. Okay? Here is Bradley Uber, who was on Bloomberg's campaign, Blagojevich's campaign coming together with a guy from India, the brains behind the votes -- the app that was developed -- that Bradley is financing to put this pilot project on.

And he's coming to it because of -- Indira Gandhi being assassinated in India and the Sikhs were forced to vote at gunpoint. And he wondered, how can we have somebody vote and send a signal that it's a coerced vote?

That's what drove him into the technology area. Think of this.

A Republican, a Democrat, a guy from India all coming together to make American democracy stronger by giving people an opportunity to vote because they're serving overseas. That's what's going on. And what I love to hear from the spokes person for Bradley Tusk, in Charleston when we announced this -- we had the two-county pilot probably in May and it worked great. Four different audits to this whole process. All the other stuff, it all came out roses, so we expand it. 24 of our 55 county clerks said we want a piece of that because we want our soldiers to be able to vote that way. She came to Charleston and said, "Look, this is what happened in the Uber world. People stood up and say, we can't go that direction, but once the people tried it, it was a momentum." And it wasn't going to be stopped and we all now benefit from having Uber in so many places. We will have the same thing with this mobile device. I'm not

proposing that it go mainstream. It's a specific solution to an identified problem.

For giving the right to people to vote who overseas serving us, that's the reward, and the risk is minimal when you start looking at the blockchain technology.

I listened to a Fox news broadcast just yesterday, and then it was filled with all the theoretical, what could happen, how -- mobile devices are insecure, and blockchain could be hacked -- folks. We're banking on our mobile devices. We're shopping on them. Sending our credit card information across them. If it's insecure, it's going to be insecure for voting, but if you use that to shop and bank so forth, I think we should be able to trust soldiers overseas to vote. And if those 24 counties that we have in West Virginia that are doing this, there are 999 different ballot styles.

Do you think somebody's going to be able to hack in from Russia into your private device, signing in with a thumb print, taking a selfie, and validating it with another thumb print to break in and identify the specific precinct ballot in the county of West Virginia to try to change one vote?

No, folks. The biggest threat, Stalin said, is not who votes that count but who counts the votes. Today it's one more who reports the votes. They're breaking into Fox, CNN, Twitter, and because they want to change the outcome. How will we put that genie back in the bottle if somebody said Hillary Clinton wins?

That's the risk of hacking into a county in West Virginia to change one person's military vote, I'm not concerned about. Yes, I'm concerned about it, but there are so many different layers. It's much more secure that you know taking a paper ballot, sending it overseas, sitting in a dusty mall room until the circulatory is able to pick that up, vote it, find the stamp and sign it, leave it back in the dust e-mail room until somebody puts it on a plane to ship it over.

Folks, when you secure a vote with a blockchain, it's much more secure.

One final thing. On the paper ballot, the voter verified aspect. We solved that. As soon as you vote, it goes into the blockchain and an email goes back to the voter so they can verify how they vote and other comes to the Secretary of State office. It's like any other electronic transmission of a ballot. There's a code on it so it's not identified by person. It's secured in a lockbox, and it's open on election day, if there's -- if there's a question, if there's no question, if everything measures up, then it's there for an audit if need be. Folks, let's say what is really there and not just argue about the theoretical. Let's talk about the reality that we give soldiers across the globe and civilians the right to vote, and let's give this pilot project a chance to work. Thank you so much.

[Applause.]

>> CHRISTY McCORMICK: I can attest to the issues you're talking about. It's a being concern. And Paul, you have a large number of HAVA voters in your district. How do you on and off they have access to the ballot?

>> PAUL LUX: Okaloosa County, a lot of folks say, why is it sitting up here? You're not Miami or one of the largest counties out there. But Okaloosa, 135,000 registered voters, home to the largest Air Force Base in the world, and we have the 33rd fighter wing, joint between the Apple, Navy, and Air Force, and we have the headquarters for the Air Force special traces command, Duke field, and on top of that, seven special forces group airborne, the US Army ranger camp, final stage of training for US Army rangers, the Navy ordinance disposal school, so we have all five service branches in our little -- our little rectangle shares the northern border with the state of Alabama -- have to say Roll Tide, sorry -- not sorry. [Laughs.]

But we share our northern boundary with Alabama, southern with the Gulf of Mexico, and one-fifth of my voters are either military or military family, whether they're in my county or whether they're out of my county.

Fully one-fifth are military family and that's how I got there. Army veteran myself. Met and married my wife. She stayed in, I got out and I followed her. I've been on active duty, a reservist, and military family and seen the problems that military people face when it comes to voting challenges.

So engaging the community is of vital importance, especially when you have the numbers that we have in our county. Of course, not everyone who was stationed there registers to vote in Florida, but Florida being a tax-free state for state taxes entices a lot of them to vote there.

We have had challenges with the assistance program on the Air Force Bases, and they have worked around most of those, and we've got a really great team in place now, but we reach out to the military community during armed forces registration week, typically in June or July. We are there for armed forces voter week going on currently I've got focus -- they're still in bed right now, or maybe not, but they will be going to the base today to help register our military families. The seven special forces group does red empire week, an open house for them when they invite the community to come and see what the special forces teams are doing, as well as the US Army rangers also do open house.

One of the things Eglind has done that has improve their VAO program drastically is putting the VAO job in among the family readiness center so they make sure the people are there to have the information, and they make sure that families have what they need while their service member is deployed and also in charge of the newcomers' briefings. Once this election cycle is over and things are back on an even keel, we will be permitted to come on base and be part of the newcomers briefing so we can reach out to folks right as they're coming into Florida and one of the things that I'm most proud of, we had a law in Florida that allowed for late registration, but the things you would to accomplish to be part of this process were very, very -- it was only for people who were leaving the service, coming from overseas. It didn't deal with deployments at all, and in 2016 I had a battalion of special forces who came back after the book closing who were not able to vote because they were too late to

register. I was happy to work to change the state law to extend the deadline to include everyone returning from deployments overseas which has impacted and improved access in the community both with the seven especial forces and the AVSOK community.

Ballot access is always an issue, and we have laws in place to ensure ballot access. Notice of elections go out annually and we send them out whether they're state, federal, or local. We send notices of elections because they don't see the ads or the campaign signs that are normal clues to people that there is an election coming, but some locals still miss t but we also of course have the obligation to mail 45 days prior to an election and we maintain that in my jurisdiction for both federal, state, and local election and we typically exceed that deadline by five to seven days. We try to get them out 50 or 52 days early if we can. Emailing blank ballots, Florida has been front and center. We originally started doing this as a response to one of our biggest challenges, which is the hurricane season, conveniently coincides. We were already mailing or emailing ballots to voters who were absent from the jurisdiction in the military, as part of that, so when it became mandatory, we were kind of like, eh, no big deal we've been doing that for years.

As Commissioner mentioned, when it came to the EAS1 and 2 grants, I was jump on let's get involved with this money.

With the federal voting assistance program.

And in our jurisdiction, we put together a consortium of 34 counties that are using -- and some of the use has come does and gone but we called it your mission, your vote, and the ballot portal has been there since 2012, so better than half of the 67 counties in Florida were part of our organization, and we used it to upload -- and part of the best practice for using this system is I asked my members to upload all of their military and overseas members into the database as eligible people, rather than awaiting a ballot. And it then becomes a poll system rather than -- a pull system rather than a push system. Their data is already there. When they want to use it, they can log in with their credentials and use the system and it includes an online ballot marking tool that allows them to generate a electronic ballot. Florida does not allow email return but they can use e-fax facilities to allow us to get their ballot in by fax or if they have printers they can do it by mail.

The other thing that we did when it comes to ballot access with the military, and again, it was an initiative that I was happy to push very, very stringently, was to expand the voting use of the federal right and absentee ballot to all of the races. They vote for everything, state, federal, and local. But our biggest challenge remains, as Secretary Warner very clearly illustrated, the actual return of those ballots. The guy in the fox hole does not have a printer or a fax machine. And we continue in Florida, I'm watching the West Virginia project carefully because we continue in Florida to need better solutions for electronic ballot return for our military in Florida. Thank you, Commissioner.

>> CHRISTY McCORMICK: And now to Sherry Poland. Workers play a huge role in serving voters on election day but they don't just show up and video that morning. It takes a great deal of ingenuity and

time to recruit, train, and oversee poll workers. Hamilton was awarded an EAC Cleary for his poll worker program. Tell us about your youth at the booth and partner in democracy initiatives and the impacts these programs have made.

>> SHERRY POLAND: In the state of Ohio, 17 and 18-year-old high school seniors are eligible to work the polls on election day. They are compensated for the work the same rate as their adult counterparts, $181. For high school seniors that is a good paycheck for one day's worth of work. We do not sign them to manager positions but they did a tremendous job in processing voters. We first initiated the program in 2007 and had some success with it back then.

But in early 2016 we saw the need to ramp it up, and that was due to the implementation of electronic poll box. We implemented in 2015 and some of which our poll workers struggled with the technology. It's basically an iPad or a tablet that took the place of the old paper books where voters would come in and the poll workers would look up their name is sign them. There's been benefits to implementing the electronic poll books, but our poll workers struggled a little bit. So we thought, who's more comfortable with today's technology than teenagers?

They have a very high comfort level with the iPads and tablets. So we needed a way to really develop that resource and recruit more of them.

So we came up with the idea to have a youth at the booth challenge, to expand upon our youth at the booth program. We coupled with a very popular pizzeria, and promoted it. The high school that provide the most high school seniors working the polls based on a percentage of the number of high school students -- we didn't want to, you know, discount the smaller schools in any way -- would receive a pizza party and acknowledgement on social media, we would do a press release. My staff and I attend the pizza party and award them with a plaque.

And in that very first year, Wyoming City High School won. And the government teacher there was extremely engaged, and I think that's really important. Because the more the government teacher is engaged, the higher recruitment you will get from that school. And she had the great idea to hold it on inauguration day, since these students had just worked and helped to administer the Presidential election. The inauguration was playing on the big screen. Afterwards, we went into the gymnasium. And then we presented them with the award. And it was a good experience for those kids and I asked them to challenge their junior class to hold their title the following year.

And guess what. They did. Wyoming won again in 2017.

There's another consume coming close to them. They might have a bigger challenge in 2018.

But the end result of all of this, we now average 330 high school seniors working the poll, almost 15% of our workforce and it's made for the perfect team because we have younger generation with their comfort level of today's technology, and we partner that with our experienced, seasoned poll workers, their adult counterparts

welcome the high school students. They're able to quickly process the majority of voters on the electronic poll books that leaves the adults to handle those voters that might be experiencing problems and work them through the process.

I think the program's not only a benefit for boards of elections and filling our positions, but we also hope that it sparks an interest in voting and civic engagement from an early age.

We also have another recruitment program, partnered in democracy, and that's where we reach out to other government agencies and businesses and ask them to partner with us and give their employees the day off with pay to work the polls.

We also have had success with this. It started out with our board of county commissioners. We went to them, explained the problem that we have in recruiting poll workers and we have the great resource of county employees that we would love to tap into. Our commissioners were the first to adopt the poll worker leave policy, and it was an easy sell to the rest of our elected officials in the county.

We have employees from not only the board of county commissioners but the prosecutor's office, public defender's office.

We also have several local businesses that have partnered with us. One of Cincinnati's Fortune 500 companies provided a little over 20 employees.

They took it a step further, after the election, they conducted their own survey of the employees' experience in working the polls, and then they shared that feedback with us, and I brought with me a quote from one of their employees. I thought it was very interesting. The employee stated, "I've been with the company for 12 years and I would have to say, this was one of the most positive and proudest experiences to date."

So that was that employee's experience in working the polls on election day. We use that quote to then go out and try to recruit other businesses to partners with us, or individuals who may be on the fence at working the polls. We know it's a very long day. But this is the type of experience you can have.

Recruiting poll workers, there's no finish line just like we talked about with cybersecurity. It's an ongoing challenge, and we do have a few other ideas that we would like to implement next year that we're still working on some of those details for the future.

>> CHRISTY McCORMICK: Thanks, Sherry. Great ideas there.

Secretary Williams. Serving voters also means making sure they have confidence in the voting system and the end results. Colorado has been a national leader in a practice called risk-limiting audits, which we heard a little bit about this morning. It's gained a lot of national attention. Could you please tell us a bit about this program and how you're using it to serve the voters of Colorado.

>> WAYNE WILLIAMS: Yep. [Cough].

It might have been a late night, but happy Rocktober, everybody. With respect to the senator from Minnesota, this is the election assistance commission -- election administration and voting survey. You will see that, yes, Minnesota is high, but they are #2 in voter turnout, not #1. Because CO stands for Colorado. Yeah, well, you

know. Rare error up there.

So why does Colorado lead the nation in turnout? Why -- with respect to my friends in Minnesota -- and more importantly, let me talk to the realities of today's world.

According a recent NPR survey, 46% of Americans think that votes will not be counted in this upcoming election. 46%.

34% think that election officials will tamper with the results of the election.

32% think a foreign country will tamper with the results of the election.

38% think that state election officials haven't done very much or nothing at all to prevent foreign interference.

These are staggering numbers. And they don't reflect the reality.

And so I want to talk about a way that Colorado has approached helping to resolve those concerns that more than a third of our nation has with respect to the elections process.

And to answer the question to the 38% to say, yes, we have done a lot at the state and local level to address these issues.

When I became Secretary of State four years ago, that was after serving as a local election official. That was after serving as a member of a canvass board, as far back as 1997 with the old punch card ballots. And there's two goals for the election process. One, to run it fairly and accurately, and the other, and just as important in many ways, is for the people to recognize that it has been done fairly and accurately. So it's just not just a question of can we convince ourselves. The issue is, can we show other people? Can we show the citizens of our respective states and the nation that the election was conducted accurately and fairly? That's what I've been focused on and that's where Colorado's risk-limiting audit comes into play.

Let me briefly explain what it is. You have to have paper ballots you can actually audit. This is an important step, in proving that Colorado in the past, before I became secretary, had a paper trail but not actually a paper ballot. The memory card for touch scenes was the vote. I adopted new standards that required an actual paper ballot, something a voter can verify, and make sure that the touchscreen didn't alter anything or the ballot marking device didn't change its programs, because the voter can look at it themselves.

And what happens after the election is that we randomly select ballots from across every single polling place and every single voter and across every single county to say we're going to audit a certain number of ballots. And we tell the county clerk, by the way, this number, the closer to the race, the more ballots we audit.

This number varies with the closeness, with the size of the county, and we then tell the county clerk, by the way, these specific ballots chosen through an open source software that we've made available to others who want to use it, to enhance it. Actually using the $360 million, our Colorado's portion, we're enhancing that software right now to make it even better.

Colorado's portion being 6.3 million.

And then we tell the county clerk, go we can't be the third box of ballots, and grab the fourth and the eighth and the 32nd out of the box and grab the fifth box and grab these specific ballots. This differs from the types of audits that had been done in the past. In Colorado, for example, we said grab a certain number of ballots, run them through a machine and make sure it counts them the same as what the overall results are.

This is an individual ballot review, where we pull specific ballots, and not just from some precinct or a randomly selected precinct, but from every county with that entire universe of ballots. And we then have a bipartisan team of judges review that specific paper ballot to see if it matches the results from the cast vote record of that machine.

We've done this now for two elections. 2017 coordinated election, which is our November election, state, local races are, and then a 2018 primary. Every single county in the state passed. Now, let me clarify a couple of things. First, you don't have to have the exact same voting equipment. One of our large counties has chosen a different vendor than the rest of the state. It worked on their equipment as well.

So it is not something that requires a single, unified system. You do have to have the ability to have paper ballots to review, because if I tell you "Go find a specific vote," you need that paper ballot as a part of that process.

So here's the reality. In Colorado, we have a way of statistically proving, of showing with statistical certainty that nobody in Moscow and nobody in Beijing and nobody anywhere else in the world changed a single vote in the election. This, to me is a critical thing not just for the integrity of the process, but so that the people know that the election is conducted fairly.

So that they know that whoever won and whoever lost, those were the actual results.

That's the fundamental basis of the democratic republic in which we live. We have to trust those results. And when I see a survey that says a third of the people think someone's going to change results, that's something that we can't sit back and say, "Yeah, but we're doing a good job." We have to come forward affirmatively and say, here's the reality.

By the way, all of those ballots under Colorado open's records laws and some reforms I helped champion are public records. And so they are available for people to review afterwards. If you don't like our risk, you can sit there in a room and count them yourself.

But it's that ensuring that people have that confidence that is something I think we need to do as election officials.

There are different variations that can be among different states but I join the Senators that spoke earlier in saying, yes, I think you need a voter verifiable paper ballot with one exception. As both of my colleagues have talked on the other side of the table here, there are some people who don't have regular mail service.

For example. I was at the ... kickoff, the inaugural -- other process and the christening of the USS Colorado, the ballistic submarine. They do not get regular mail purposes, which defeats the

purpose of stealth if once every 24 hours you have to come to the surface to get mail. So there has to be a process for individuals who serve there who protect right to vote to have the able to vote. And there's a small number, and Colorado has an encrypted return option for individuals who serve on a nuclear submarine or other circumstances. But for everybody else, that ability to have a voter verifiable ballot is critical and it provides us a way for telling people, yes, nobody anywhere changed a single vote in Colorado or elsewhere in the nation.

>> CHRISTY McCORMICK: . Thank you. We're going to go to questions from the audience, and since we're short of time, we have other questions. But to reiterate Commissioner Hicks's rules, speak into the microphone. Give us your name and your affiliation. And please ask a question.

So we've got microphones. Who has questions?

>> AUDIENCE MEMBER: Mark Schneider. This question is specifically for Secretary Williams.

Prior to implementing risk-limiting audits, what were your expectations in terms of cost, level of effort, et cetera, and after doing that, did you find that it was less than your expectations? Greater, the same?

>> WAYNE WILLIAMS: Thanks for the question. If you did not have a cast vote record as our new systems do in Colorado, it would probably be a more costly method of auditing.

But with the newer systems and the cast vote record and the ability to pinpoint specific ballots, it's actually lower cost in most elections. And I say in most elections, because the number of ballots you pull varies. If you had an extraordinarily close election, it would be more costly.

I would submit that if you have an extraordinarily close election, it's worth spending that extra amount to make sure you have the right result.

But overall, it's resulted in an easier process and a quicker process in most elections.

>> CHRISTY McCORMICK: Other questions from the audience? You have one up here? Back there? Okay. Go ahead.

>> AUDIENCE MEMBER: Eric Fisher. There's been some talk about having more rank order ballots for close elections, where you vote, you know, you choose an order of people, and I wonder if you've considered that, what is the advantages and disadvantages?

>> CHRISTY McCORMICK: Rank choice voting? Anybody have questions on that?

>> One of my biggest concerns, I, like many panelists before me, have the certified election registration administrator certification from the center at Auburn University, and one of the things they did for us and one of the follow-on classes after you do the certification, they give us the same set of ballots and they asked us to count them one by hand, and two, using various other methodologies. And of the number of different methodologies of rank choice voting that you can choose, counting the same stack of ballots seven times came up with five different sets of answers, which concerns me and why I'm not a huge fan of rank choice voting.

Understanding the reasoning, but for me personally and the colleagues, that's always been my biggest concern.

>> WAYNE WILLIAMS: Colorado recently adopted rank choice voting rules. We do permit it for certain local elections.

But there are some interesting questions, and I'm actually convening a working group following the election to address some of those. Say there are five candidates running and A and B I really like, and E I absolutely hate. So I write 1 and 2 by A and B, and I write "dead last five" by E, but I don't know the other two, C and D, so I leave them blank. How do I count that ballot?

There are different methods of rank choice voting, some of which say you skip over the blank ones, and my last dead last choice becomes third. Some say it ends if I skip.

So there's a lot of issues that have to be resolved, because not every voter will follow all of the rules and guidelines that you issue. I know that shocks some people to hear that.

[Laughter.]

Show of hands. You're an informed group. How many of you read the complete voter instructions in your last ballot packet?

Five! Six! Great! Full room. But I think it illustrates that -- or in the voting machine, or anywhere else you were at -- that lots of people may not read all the instructions, and so there are a lot of things to look at. It has some appealing opportunities but there are questions that have to be answered so you get consistent results, and that everybody knows what those rules are going to be.

>> CHRISTY McCORMICK: Next question? Got one here, up here. Sorry. Get that hand high.

>> AUDIENCE MEMBER: Elections council in the house committee on administration -- my question is for Secretary Warner. I'm excited about the mobile voting prospect, and I want to know your concerns about election security, if it's good enough for banking, should be good enough for voting. And in the same vein, do you think the eventual goal should be to move in that direction, and if not, why not?

>> MAC WARNER: Thank you for the question. Great concerns. What we're hearing an awful lot is back to the theoretical. That this could happen. Until it does happen, I'm willing to continue down the risk-reward trail. So many people if they would just pick up the phone and call the office. If anybody in the room has questions, see Don. He is the brains behind all of this. And that opportunity right now to talk to the guy that's responsible for this.

The -- and, folks, we're learning. That's why it's a pilot program. We're starting small. A dozen or so that voted in the primary. And from that, one of our clerks came to us off the bat and said, "You got to get a paper and verified trail so the voter can look at it." And we worked on that between the primary and today, and the email, as soon as you push vote, the vote goes into the blockchain and another email goes to the voter and he can print it out and we get a copy in the Secretary of State's office. You have three different opportunities to verify, and if there's a question with any of it, we'll go with the paper ballot.

So those are the issues that we're dealing with, improving it as we go. I'm looking for this wider audience in the 24-county situation. Folks, we've already had people already, right now in this election from 8 different countries, Philippines, UK, Mexico, all of those countries, I'm talking about these people, State Department, and instructor teaching overseas, a student in China or whatever. Everybody has an opportunity to participate.

So those were some of the issues we're dealing with.

And it's been nothing but positive, by people -- West Virginia Air Force pilot that said I was able to come back and vote, and his wife said, thank God for this, I have two children under two, I voted between feeding my two children in the kitchen.

That's the responses we're getting from people.

And so back to your question to the broader audience, I'll let other people take in that direction. I know other states are looking at it with other rationale, and they will have to do the risk-benefit analysis. As long as people have the right to go to the ballot box, or the opportunity, I think there's value in waiting until election day to do that. You saw what happened with the FBI and all these -- Wikileaks and so forth before the 2016 election that happened in the last 30 days, or the last four days. There's a benefit to waiting until election day. I'm not looking to take it to a broader audience, at least not until we've proven the whole technical aspects of it and the process of it, and the acceptability.

>> CHRISTY McCORMICK: Question up here.

>> AUDIENCE MEMBER: I'm Cole, a civics teacher, served on the HAVA committee a million years ago. Director Poland from Ohio, as a civics teacher I'm looking for ways we can engage the next generation of properties. And to use the military analogy, if I take a bunch of children to the flight line and say, if you learn how to fix this for two years you get to fly it.

I'm looking at, how can we expand this as an educational opportunity.

The models are what I'm looking at, how is that delivered? How is that training done? They're used to a certain way of education. Not every election official teaches, if you will, all the time. So that's a different kind of a skill set. The part I'm looking for, perhaps in Ohio like we're going to do in Minnesota, pairing up high school students with military veterans for the training. They sit next to somebody who knows something about service and training.

The upside, that's what I'm looking for, West Virginia is uniquely placed, you put the 26th Amendment over the type that gave them the right to vote. Do you have a specific role that under18-year-old students could take a role in the election and be of service to their country?

>> SHERRY POLAND: Yes. As I mentioned earlier, 17-year-old voters are not only eligible to work the polls, that's younger, but they can vote in primary elections, as long as they're 18 before the general election.

>> PAUL LUX: And one of the things that our HAVA security is spent on is improving online training platforms and we hope -- in Florida we have a requirement for a minimum of three hours for

experienced poll workers, and a minimum of five hours for new poll workers, and if we can eliminate all but one hour of that training by an online platform, it will drastically improve my ability to reach that demographic. As a preregistered voter you can serve as a poll worker at 16 or 17. And we do have high school students in 2016 who were able to get time off from school. I'm really terribly interested in the program there in Hamilton County because he would like to see more and more. Like Secretary Wyman, I think the average age of my worker is 65 to 68 already. But that's -- absolutely. Oh, no question.

>> WAYNE WILLIAMS: Thank you. The 26th Amendment started when president Roosevelt lowered the draft age but not the voting age.

And when he finally did in 1971, the first person he registered to vote was Ella Thompson, an 18-year-old. Her brother had been killed in Vietnam without ever having had the chance to vote.

So it's a poignant lesson in West Virginia, and we take pride in this effort to get young people engaged in the process can, so accordingly, we take a Jennings-Randolph award to the high schools who register 100% of their eligible students to vote. And it's grown and we have 39 schools that got it this last year. 100% of their eligible students to register to vote. And we have the youngest delegate elected to a state legislature in the history of the United States, Sarah, a 17-year-old when she was elected and turned 18 when she took office.

My message is, each of your states has somebody who's championed youth involvement. Find it, name an award after them, and get out to the high schools, and people will rally around. It's catching on in West Virginia. Thanks.

>> MAC WARNER: In Colorado we have a similar award. And we have student judges with a slight variation. One of our counties has partnered with a school district, and they close the schools and allow them to be used as polling places, and the student judges designates which of the school activity funds they want the money to go to that would normally pay an election judge and that's been popular. The school received a NASS medallion for the program because it gets kids involved. Instead of selling beer at a baseball game to try to raise money for your activity, you're working an as an election judge. And the amount you can raise in a single day can really help some of the activities at a high school.

>> CHRISTY McCORMICK: Thank you all. We are going to take a -- I wish we had time for more questions. You could ask questions all day. But we will take a 10-minute break now. Please come back at -- to this room at 11:45 for a discussion on security, national security with the director of the office of national intelligence, William Evanina, at the Department of Homeland Security, Chris Krebs, and Jim Condos.

So we'll see you back here.

>> Quick announcement. I have a few papers with the stats I mentioned earlier. If you would like to pick one up, please do so.

[Break.]

>> Ladies and gentlemen, our program will begin in two minutes.

Our program will restart in two minutes.

>> Ladies and gentlemen, please return to your seats. Our program is about to begin.

>> Ladies and gentlemen, please return to your seats. Our program is about to begin.

>> CHRISTY McCORMICK: Welcome all, back from break. If you could take your seats, I would appreciate it.

So our final discussion today is focusing on national security, and our panel of experts is hard to top when it comes to this topic. Joined me today are to my right, William Evanina.

An organization he has led since June 2nd, 2018 the director serves as the head of the counterintelligence for the US government and as the principal security advisor to the direction of national intelligence, leads the security activities of the US intelligence community, the US government, and US private sector entities at risk for intelligence collection or attack by foreign adversaries. Under his leadership, the national county intelligence and security center -- foreign intelligence threat awareness and closing critical security gaps in executive branch departments and agencies, and I thank you for joining us for this conversation, director William Evanina.

Next is Christopher Krebs, the undersecretary for the Department of Homeland Security's national protection and program directorate, I think I heard you -- [speaking away from microphone].

But it's the NPPT. As undersecretary, he overseas NPPD's effort to continue the networks, secure federal facilities, manage systemic risk to critical functions and work to raise the security baseline of the nation's cyber and physical infrastructure. Before serving the MNND, he served as secretary for infrastructure protection, joined DHS in March of 2017, first serving as senior advisor to the secretary.

Prior to coming to DHS he was a member of Microsoft's US government affairs team as the director for cybersecurity policy, where he led the work on technology issues. Before Microsoft, Chris advised industry, federal, state, local and government customers on a range of cybersecurity and risk management issues, and prior to this, served as the advisor for the secretary for infrastructure protection. He's also a fellow graduate of George Mason University School of Law. Welcome, Chris.

And on my left, Vermont Secretary of State Jim Condos, getting involved in government to help a local zoning issue, read up on statutes, and has been an advocate for transparency. He's served on the south Burlington city council.

Since his election of Secretary of State in 2010, he's worked tirelessly to bring transparency, and the current president of the national association of Secretaries of State. He's been active on voter participation and cybersecurity, testifying before the US Senate rules and administration committee to discuss what states are doing to secure elections from cyberthreats and attacks. Thank you for joining us.

So I'll start on my right with Director Evanina. There are a lot of federal agencies involved in national security and each plays a unique role. Your agency is not always on the front page of

election security news. Could you tell us, please, what role your agency plays in helping the federal government and states to secure elections?

>> WILLIAM EVANINA: Thanks for the opportunity to be here with the esteemed panel. I think it's a good thing we're not on the front page every day -- but I think your point is valid. You know, when we look at the auspices of what the election process means to us, as a democratic republic and the electoral systems, it's a call to arms with respect to everyone having to play in the space. Specifically with NCSC under the auspices of the director of national intelligence, our job toto provide real-time threat and warning to the folks who have to implement these processes, primarily the FBI and DHS. What is the most efficient and effective manner we could take real-time threat information from around the globe, wash it through the washing machine, called the intelligence community, and get it to DHS? So they could effort it and get it down to the folks who every day with the process. We are building an apparatus that we have not had before and takes a day by day approach with the excitement, with the midterms, and we've a lot of to learn from with respect to the 2016 election.

So under the guise of the intelligence community, NCSC role is to garner all of the intelligence and for that we can for anybody who is a policy decision maker what the real-time threat information is, so that we could implement it on the ground floor.

>> CHRISTY McCORMICK: Thank you. And Chris, the designation of elections as part of the nation as critical infrastructure after the 2016 election was established to provide new resources to the states and improve communications. Both among federal agencies and between the federal government and the states. How much time designation had its intended effect what and what do you see as the most tangible impact of this work thus far?

>> CHRISTOPHER KREBS: I wasn't around in January of 2017 when the designation was made, and when we talk about improving communications, I got to admit, in the early days of this administration, there was communication going on between DHS and the states. I wouldn't say it was good communication.

[Laughter.]

My metrics of success were pieces of mail.

And I got a number of love letters --

[Laughter.]

And Secretary Kelly got a number of love letters, or hate mail, however you want to describe it. Describing the way that the process had rolled out. Communication was not a key element of the initial rollout. And really when I look at where we are right now, the single most important factor that has been established between DHS, alongside EAC and the intelligence community with our state and local partners is trust. That's the keyword. That's what we've been able to develop with our partners. And it's important to kind of work through why that's significant, because back in 2016 when the phone calls were made, saying, "Hey, look, we're seeing something. There's something go on in your network. I need you to take action. By the way, you have no idea who I am and you've never heard of NPPD, you've

never heard who the leadership was at the time, but I have been you to take this action." There was no trust, and there was no certainty or confidence in that ask.

Now, we have done a number of measures, including establishing information security analysis centers focused on the state community where we push on the threat -- we have communication protocols, accord coordinating messaging, unity of message, and it's a completely different ball game. When we think about sharing information that means from the DNI, we have processes in place. We have security clearances out to the security officials, but even without that, I'm confident if I had a piece of information that Bill passed to me and I needed to call Secretary Condos or any other Secretary of State and say, "Look, I got something you need to say and take action. It will take me a day or two to get to the information but in the meantime you need to take action." We have trust established, and there would be the beginning of an article of faith that they could do action and we could get that piece of information out there.

>> CHRISTY McCORMICK: It takes time. And I think, you know, I'm not sure if everybody was on the same page over what the intended effects were for that process, and I think that's developing. And, you know, appreciate all the work that you all are doing to communicate on your side to the states on the other side.

Speaking of states, Secretary Condos. As Vermont Secretary of State and the president of NASS, you know a lot about the challenges facing the states and the resources available to help them navigate these issues. Where did things stand? Do the states have the support they need to secure elections in 2018 and beyond?

>> JIM CONDOS: Thank you. I think first, let's -- I'd like to reflect back to August of 2016. And just -- not to talk about the rocky start. You've already heard that story. [Laughs.]

But what I think is more important, was that there were 21 states that had been attacked. And of those 21 state, only one state was actually breached. Yet all the discussion in the media and, by the way, I do trust the media -- but all the discussion in the media had to do with the one state that was breached. There were 20 states that were not breached. There were 20 states that defended well. And that's a story that's been missing in some of this discussion.

Having said that, I will say that we are -- we were in good -- we were in fairly decent shape back in 2016, but we are in much better shape across the country in 2018.

And we'll be better even more in 2020. But I think it's important to just recognize that this is an ongoing, as you heard earlier, it's a race without a finish line. There is no end in sight. This is going to be the new normal for us. We have to focus and work with our federal partners. We are working with our federal partners. DHS is providing many resources to the states with regard to penetration tests, with vulnerability assessments, cyberhygiene -- we do a quickly cyberhygiene test with them of our system since August -- or probably fall of 2016 just prior to the election.

And it's been ongoing ever since. I think that we have to stay vigilant. We have to maintain -- or stay ahead of the bad actors and

that's not easy to do, because let's face it. The bad actors that tried to get in yesterday are going to try a different way today, and they'll try a different way tomorrow.

We have to hope that we've got the defenses in place to block them.

And I know, you shared with Jeff a -- I shared with Jeff a diagram from our office, from our ID department where we've been averaging since last June approximately 2 million hits a day to our system.

Now, that sounds like a lot. And it is.

But only about 800,000 we've been able to identify are actual what we think are threats. But we're blocking them. We're stopping them. They're not getting anywhere near the system. And that's good news. We're doing our job, putting the right things in place. We have redundancy and resiliency. We do a daily backup of our voter registration system. We also have same-day voter registration. Even if someone were to get -- if the worst happened, and the bad actor did get in, we would still be able to get everybody that wants to vote on election day to vote.

So that's -- that's the good thing I think that we've been doing. But from my personal opinion, not NASS's, my personal opinion as Vermont Secretary of State, what we do need is ongoing, sustainable funding to the resources to do the job that we have to do in this new world that we're in.

It's nice to get the money. It was $3.9 billion that was approved. Only $3.6 billion was appropriated from 2002 HAVA. That was hanging chad money. Now we're thankful the $380 million passed. It was the remaining portion of the money but they changed a few things to allow for cybersecurity use. And I think that that's been good.

And then but going forward, we could not -- the states will have a difficult time meeting this challenge if we have to depend on once every 10 or 15 years getting a lump sum. We need sustainable, ongoing funding, one a year or every two years, that's up to Congress to decide, but we do need to have some kind of sustainable funding going forward.

My last comment before I turn it back to you is the EAC.

And the EAC to me is an organization that needs to be fully resourced. It need a full complement of commissioners and staffing and resources to do the job that they have been assigned to do. They have not been able to meet that test, because, mainly, they don't have a full quorum. You guys can't even meet -- discuss things, because they don't have a quorum of their commissioners.

The staffing has not been -- could be better. But I will say this: They know what they're doing. The EAC can help the states. It is the one organization that can really help us, in addition to DHS, but it's the one agency that can actually help us, because they're involved in the elections assistance for the states.

So I guess I'll just leave it at that.

>> CHRISTY McCORMICK: Director Evanina, what do you think poses the biggest threat, and how to prepare?

>> WILLIAM EVANINA: If I can rephrase the question to biggest

threat to the election process. When you're talking about systems, Chris can talk all day about the system, what the system is and isn't, but I look at it from a broader perspective with the threat to our democratic society and values and what voting to us means as a democratic institution as the best in the world. And I put it in two buckets. The first is the cyber threat to the electoral process. And that's the systems that every single precinct, location, and Chris can talk about all of that and what that means when there's an attempt, a breach, an exfiltration or just an event, what that means to the actual systems infrastructure, software, hardware, supply chain, all of that stuff is in one bucket.

The other bucket which I concentrate more is in the influence of our adversities. What they're willing to do and we can't forget what happened historically, in 2016, with the efforts of the Russian intelligence service, plenty of indictments, what they did with not only manipulating Facebook and other social media enclaves to attack and influence our hearts and minds as voters. And what that means.

So I think when it comes to the threat, it's a combination of actual physical cyberthreat and also the maligned influence that not only our adversaries, but others that wasn't state sponsored like Wikileaks, and it's -- and how do we combat that as a country, as a whole society prospect, how do we push back and understand social media and in the media and what it means and doesn't mean, and can we think objectively as we move forward with the electoral process and be able to vet fact and fiction and understand who's proceeding the message and can it be a foreign country that's trying to influence a voter or a group of voters or a state and what does that mean. There the most secret and the President and the DNI have been clear about foreign governments who have interest in particular candidates. That's not a secret, and it's not been a secret to us. How do we vet that intelligence out, provide that objectivity voters? When it comes to threat, it's the threat of cyber and also the maligned influence that we face in the intelligence community, real life, what does this mean and how does it impact to the American voters.

>> CHRISTY McCORMICK: When the President was at the UN he said that the Chinese were attempting to infiltrate our 2018 elections. What can you tell us about that? Anything at all? I mean, is this something that we as election administrators need to be, you know, concerned -- I know we have to be concerned about any kind of foreign influence, but ...

>> WILLIAM EVANINA: On behalf of the intelligence community, the President was right with the comment with respect to it's not just Russia. Right? Russia is a shiny object, because they've done that, but China is heavy in the influence process with our electoral process. Specific candidates. And now with the play book being set, any foreign government, Iranians, North Koreans, anyone in South America who have the ability to promulgate -- and the quote has been that China is also influencing how we look at this process, and they have interest in particular candidates that are pro-China or pro-Russia, and they promulgate efforts that could help them win the election.

>> CHRISTY McCORMICK: Do you think this is more social media

oriented than voting systems?

>> WILLIAM EVANINA: In my role, for sure, that the voting systems are the process, but when you go into that voting booth, the foreign entities try and influence you before you get into the booth.

>> CHRISTY McCORMICK: Got it. Interesting.

Secretary Krebs, we know that threats to our election systems are sustained and ever-evolving. While our state and local election leaders have put in place necessary steps to protect election, they still may face an incident.

What is the play book or chain of events that would transpire if an election official suspects they've been targeted?

>> CHRISTOPHER KREBS: Bill talk about the election cybersecurity hacking, ands maligned piece, which I break down into two parts. Think about the hacking, the DNC compromise, and they took information and weaponized it for political purposes. The second part is the information operations, and that's about organizing protests and counterprotests, driving people to a physical place and looking for conflict. Sowing discord.

So the unfortunate thing for election officials, they can't just look at one or two or three buckets. You have to look holistically. Because even if there is not an actual compromise of a machine or a voter registration database, things can happen. Technical glitches. Or somebody that pops up on a social media platform and say, "I was able to get in." Whether they did or not, it doesn't matter because it undermines confidence in the voter.

#1, crisis communication. Being on top of the issue and communicating quickly and clearly and with authority to the public. And we've seen that, and if -- we've said this before. If I've learned anything over the last year, it's that Secretary of States that election directors are just natural risk managers. They deal with technical glitches every year. They deal with robocalls that are one way or another messed up. They deal with DMV and board of elections disconnects. Things don't come over.

So we have really well-tested crisis communications plans, but now we're adding additional complexity to it. It's if you spot something on social media, how do you identify that? How do you get to the root cause and how do you communicate that out?

We're doing a numbers of things. We have the table top vote exercise in August, 44 states and the District of Columbia. Not all could make it because it overlapped with the primary. But that was the drill that puts us through the paces of, okay, here's what's going to happen over the course of the next month. The thing that we're working on to reinforce with the election community and being off of Bill's comment, when you think about the whole pie of information available on any given incident or any given event, the intelligence community only sees a slice of it.

We have to get over the assumption that the government, the federal government knows all and sees all and has intelligence collection holdings that are able to paint the full picture before a bad thing happens. It's not how it works. They have a piece of the pie. The more information that we can get from the election community, no single piece of information, no anomaly is too small.

We really encourage folks, if you see something, say something. I mean, it applies to cybersecurity too.

So put stuff in -- you know, call the NCCIC, which is where we have right now we've activated and stood up and enhanced coordination procedure with the regular flow of information, and on election day, in Virginia we're going to have our war room for election day, and we'll also have an online presence so that any election official across the country can get into this kind of web chat and if you see something, put it into the community, and it's not just so that DHS sees it. It's so that Pierce and counterparts can see it, and you can start putting together the big mosaic of what's going on there.

>> CHRISTY McCORMICK: Administrators know what the NCCIC is, but a lot of the online listeners --

>> CHRISTOPHER KREBS: Great point. It's the National Cybersecurity and Communications Integration Center, and that's the DHS critical infrastructure cybersecurity perhaps center, both for the federal government and also for critical infrastructure partners.

>> CHRISTY McCORMICK: Thanks more for making that clear. We talk in acronyms all the time. Secretary Condos, what do you tell them to know that everything is being done to protect the integrity and accuracy of elections?

>> JIM CONDOS: I have a long list of our best practices that we do, and at every opportunity I get out with people, League of Women Voters, Rotary clubs around the state of Vermont, and frankly, I just keep drilling down. These are the things that we are doing.

But I think for us, it starts really with paper ballot.

And, you know, we -- I am a big believer in paper ballots, not paper trail, paper ballots themselves. I think my colleague from Colorado mentioned the same thing.

And paper ballots, we've always had paper ballots in Vermont. We memorialized it in statute in two thousand -- I think it was 2002 or '03. I helped to be on the committee in the state Senate that moved that.

And then in 2006 -- or 2005, we passed election audits, postelection audits, and in 2006, we've started doing our audits. We've done them every two years since. And we've never found a discrepancy yet.

We changed it and strengthened it in 2012. And we have what we consider to have -- we consider it to be a strong, 97% confident level. Not that risk limited audits are good, and generally the risk-limited audit works off of a 90% plus. So we think we're in the same ballpark with the audit that we do.

And I think that was one of the things that came up that there are more than one way to do an audit.

Then we have the other things that we do. As I said previously, we do a backup, daily backup of our voter registration system. We've added two-factor authentication for anybody getting into the system, including my own staff.

To get into the management system.

So with the daily backup, we can go back 24 hours and reset our voter registration database and only lose a small amount of actual registrations. And we have same day voter registration. And we have

automate voter registration in Vermont. I think we were the fourth to pass it by legislative passage, but automatic voter registration helps us keep a more accurate voter registration database as well.

Combatting misinformation. You know, I don't think there's any good answer to that.

You know, we are constantly looking through Facebook and Twitter to see what people are saying. But we don't have anybody dedicated to that, so it's just what we pick up on our own or in someone contacts us and says, "Hey, I saw this," and we'll get on and refute whatever it is. We'll set the record straight.

We also let people know that none of our vote tabulators, none of our tabulators are connected to the intent by either hard wire, WiFi, or remote access software. And as I said, we have the paper ballots which we seal and store for 22 months. We had one group that just did a -- their own little test and picked the town of about 5,000 people, and went to that town just after the 22 months were up, opened up those bags, as a the clerk was getting ready to destroy the ballots and did their own count on a specific race that they were looking at.

That race, they had one ballot changed. In a town of 5,000, one ballot -- the vote total in their view changed by one.

Interestingly, we have had -- we do several recounts a year. And those also help us to identify if there's any potential issues.

So, you know, between that and our postelection audit, we feel pretty confident.

It is hard to get good information out there.

You know, the media sometimes -- and this is not blaming or pointing fingers, but the media is really the only way we can make sure that we get a broad stroke out there, and depending what the news of the day is, your story might not be the one that they want. And I understand that. I've been around the media for years.

But we have to -- we have to partner with our media. We have to ask them to help us get certain messages out.

Again, I talked to Rotary clubs throughout the state on a regular bases. I talk to schools, League of Women Voters, any group that wants me to come speak. It's just -- I believe in transparency. I believe in openness. And that really is the basis of what I do.

The last thing we did was last spring we held -- if you want to call it a cybersecurity summit. We called it defending our democracy. Our DHS partners were there. The FBI was there. Our local election votes focus were there. NASS was there. We had a good cross-section of folks and it was a two-hour special -- special -- it was a two-hour presentation that we did with -- for the media specifically, for our legislators specifically, to for the public. We invited everyone to come. And I think it was well received.

So I think I'll let it go back to you now.

>> CHRISTY McCORMICK: Director Evanina, we had a conversation a couple of months ago. We were talking about the propaganda issue. You mentioned all that anyone would need to do is hack one machine, but really, we discussed -- they don't have to hack one machine to affect voter confidence. How do we combat that? How do we deal with

voter confidence in the propaganda issue?

>> WILLIAM EVANINA: I think it's a complicated issue and it starts with partnerships, dialogue, and lexicon. We've done an energetic job in the last year driving partnerships in very productive manners, where we have table tops, bring in the intelligence community to advise and inform DHS of how that process works. Where do we get the intelligence from? At the same time we allow DHS to provide the intelligence community what they need to operate and do their business, truly open the eyes of the intelligence community for change. We send out collection requirements to identify threats, as well as a product to every state and local official to say, this is what we're hooking for. Partnering with DHS, the FBI, yesterday, again, we brought in the vendor partnering with DHS to talk about a classified venue, what are the threats, what does it look like, and so we have the vendors continuing to indicate and have dialogue with the DHS, NSA, all in the same room, understanding that partnerships, the through, and what is the common lexicon. What is a hack versus a breach, versus an attempt. All of those keywords matter when it comes to deciphering reality verse not reality on election day. The more that the individuals who are in the same process together understand that lexicon, the more effective we can be as a government to transmit the information to the public. When you have suspicious activity at a polling place in Alabama or Virginia or in Virginia, and what does that mean? Suspicious activity? How quick can we vet that out? That only happens through trust, as Chris said, and partnership in lexicon. We have to be on the same page and be able to sift through the noise to be able to say what is the influence what and what does it look like, and let the experts understand if there's a cyberactivity, what does that mean, and what is the reality. And if there is, does it really have an impact on the vote?

At the end of the day, our job collectively here, everyone in this room and as an American, our #1 issue so the question is make sure everyone goes out and votes. Voter confidence, we are all on the same team to make sure that voter confidence is maximized come November and any election. Our ultimate goal as a democratic society is to execute what we are given, which is our right to vote and we have to do everything we can to install that trust not only the systems but in the importance of voting as a American to combat the influence of foreign adversaries.

>> CHRISTY McCORMICK: You mentioned a number of federal intelligence agencies. How do you communicate? FBI, ODNI, DHS finds information. How does that work?

>> WILLIAM EVANINA: The DNI has identified a crisis manager for elections within the ODNI. And that individual coordinates weekly to bring together as much threat information and what's going on at the FBI and DHS, NSA, CIA, all organizations provide a common operating picture of the threat that we see every day manifested or both see and to be able to provide that information to Chris and the FBI to facilitate their investigations, but to have one voice, one vision, through that crisis manager that everyone can funnel through and get it to Chris who can get it to the everyday key components of the

electoral process.

>> CHRISTY McCORMICK: Chris, what's the threshold of when you need to communicate this information out? How do you know when it's so important that this gets out to the -- at least the state election officials and maybe even, you know, down to the local election officials?

>> CHRISTOPHER KREBS: For sure when it's actionable. When we have something actionable, we share that.

But when we have enough of kind of a baseline understanding of what a tactic, technique or procedure is for more strategic intelligence, it's not necessary something that's hitting a network but general trends we try to push that out.

To step back a little bit, and building on what Bill said earlier, when I break out the election cybersecurity piece and the information operations piece, they have two fundamentally different solution set. On the engineering side -- or on the technical cybersecurity side, fundamentally it's an engineer problem. It's a technical problem with systems, equipment, people, training, things like that. It's imminently solvable with the right amount of people, resources, technology. We can get there.

On the other side with the information operations side, it's much more human nature and it's much more psychosocial. In and that brings in a completely different set of solutions.

And so in part, it's about awareness being and resilience building. When you go back and look at the assessment in January 2017, it the way I read it, it breaks down into two different information operations styles. One is a dynamic repopulating and rebuilding style across social media platforms. Twitter handles, Facebook pages. Stuff like that.

They pop up and down. On the other hand, we have a static footprint, and that's state-sponsored media. We have to train peach people. How far on the link before you click. Same with social media. Who is this anonymous? Raise the critical thinking of social media users. But on the other side with the static, it's a -- the state sponsored media, for instance, we talk a good bit in the ICA about Sputnik and RT. What they push is what the Kremlin wants them to push. We need to just call a spade and spade and recognize that if you're getting presented something from state-sponsored media, why are they presenting it to me? What is the objective they're trying to accomplish? And do I need to click like, share, or retweet, or whatever? We really got to get much more cynical and critical about the information that's being presented to us.

>> CHRISTY McCORMICK: And if I as a citizen think I'm being targeted, how do I deal with that? Who do I tell? How do I get that information up?

>> CHRISTOPHER KREBS: This is where the shared responsibility comes into play. Between all levels of the government and the private sector. The social media companies have absolutely stepped up their game. It's been a quite impressive movement across a number of the platforms. Report. Report a tweet if you don't like it.

>> CHRISTY McCORMICK: Who to?

>> CHRISTOPHER KREBS: It's in Twitter. It's in Facebook. They

have that capability to report it forward. It helps them tailor their algorithms and this things they're looking for. It is as much right now just like cybersecurity is a shared responsibility, same thing goes with information operations.

>> CHRISTY McCORMICK: Is there a way for them to report that to law enforcement?

>> CHRISTOPHER KREBS: Absolutely. FBI and DHS will take that as well but the FBI is leading the information operation's public face piece.

>> CHRISTY McCORMICK: For all of you with regard to the federal and state partnership, what would you say is the most impactful development, going back to 2016, since sort of -- this wasn't on our radar before 2016. And what is the biggest challenge they're facing?

>> WILLIAM EVANINA: I will step up my previous answer. The dialogue between every aspect of this process. And I think the partnerships that the intel community at large build with DHS, and bringing the FBI into the fold with respect to broadening our aperture of more than just investigations.

As well as partnering with you and your commission as well as, we brought in and partnering with DHS back in the springtime to bring in all the Secretaries of State and election officials and provided them a one-day classified briefing that. Drives more dialogue and conversation, and I'm going to point to something that happened that got some publicity about then went away. The indictment by Department of Justice and FBI of IRA and the GRU and you see Putin's commitment to drive society and use our social media and our own freedoms against us, and I think that allows the intelligence community and DHS and everyone in the states to look the realm of possibility of what's going to happen next. What's the predictive analysis that we think the Russians and the Chinese will do.

The challenge is more dialogue. And we look at the progress we've made, whether from the election officials up to the federal government, but also I would say reimagining the intelligence community to look differently at how -- who our customers are.

And in terms of not only the DHS apparatus, but again, from the states and locals that we have to start collecting in a different manner from a different constituent that could use that challenges and that's the challenge. How do we do that with existing laws to protect civil liberties, but we have a duty to inform and advise those who can make decision.

>> CHRISTOPHER KREBS: I had a serious answer and a half serious answer. Hiring Matt Masterson.

The other was the 2018 omnibus, which included dedicated funding for DHS so that we could deploy additional Albert intrusion detectors, and additional assessments and established a foundation in my team for a sustainable elections support going forward, but perhaps more importantly, $380 million to the EAC to distribute.

That's the most tangible, but when you step back and you look for the intangible developments, it's been trust.

>> JIM CONDOS: So I would just follow up, Chris, by saying that the trust factor and the increased and improved communications, and I also agree, having Matt there helps us a lot.

When we first started, we were really walking, I guess you could call it on eggshells and then started walking on the beach sand and all of a sudden it became a much firmer ground, and we now know what our different aspects are, what the strengths are, and we know what's available to us to help us make sure that our systems are in good shape. And I think it goes both ways, and we as Secretary of States have to communicate back to DHS and the FBI to make sure that they're getting the information they need that we see. You know, earlier this summer, we saw -- we saw what we thought might be a potential threat, scan, going through our system, didn't get in. We blocked it before it got it.

But we sent it down to DHS and to MSISAC, the CIS, we -- we -- the center for internet security -- well, MSIASC is the multistate information sharing and analysis center, and we sent it to them, and to the FBI just to get it out there so they could look at it and say whether this was something bad or not.

And, you know, it's that kind of stuff that we as Secretaries of State and election directors have to provide that information back to them so that they can act on stuff for us.

I think a major factor that I appreciated for our primary, anyway, was the election day threat dashboard that was established by DHS so that we now have a communication tool in front of us that's real-time and we can -- we can input into it or receive input back from any of our colleagues across the country of what they're seeing out there. And that to me again is the communication, helps build the trust, but it just keeps us informed of what's going on and where to focus attention.

We also set up the EIISAC, election infrastructure information sharing analysis interest. And it was from what I've been told by the center for intent security, the faster set up of an ISAC for a specific critical infrastructure that they've ever done and we now have over a thousand members to it. We have all 50 states, six territories, and the rest of those are our local county and state jurisdictions. And that's just a tremendous platform for us to be able to provide information.

I mean, when you think about it, that's what cybersecurity is about. It's about information, making sure we've got the right systems in place, but it's about sharing information with each other.

>> CHRISTY McCORMICK: Thank you. Director Evanina and Secretary Krebs, looking ahead to the November's election and the 2020 Presidential election, if you had one piece of advice for election officials, what would that be?

>> WILL: I'm not sure on one but three. #1, trust. And using Chris's point. At some point in your future, next month or 2020, there will be a piece of intelligence that comes so fast and furious in the community, the phone call will be made to Chris that will tell him, hey, this happened and we need to act.

Chris will pick up the phone and call a state and say, you need to do something.

And you have to trust Chris. And follow up on the ramifications later. I look at this as similar to a terrorism event. The information, the flow via trust will happen first and then go out

later, and I think we're build that, #1.

#2, do not panic. If we see something on CNN or Fox, don't panic because if there is an attempt or breach or event don't panic because just because there's an attempted breach at a polling place doesn't mean there's an impact with the election. Don't panic with the news media, because at the end of the if something happens in Atlanta at 9:00 in the morning we need that to not influence the people in California.

Don't panic. And see something, say something. If you work at a polling place, you're a volunteer, and you see something that's not right, call Chris or the FBI's local field office. Don't sit on that information.

>> CHRISTOPHER KREBS: Last point. Communicate early, often, and late. No piece of information is too small. It helps us build the bigger picture of what's going on. But what may be insignificant to you could be immensely important to a peer, state, or local government.

>> CHRISTY McCORMICK: And Secretary Condos, what do you want us, your federal partners, to know as the election approaches, and what do we do to help you?

>> JIM CONDOS: We pretty much tackled it, but trust, communication, and I think as Bill said, when we have the -- when -- we get that phone call, we have to act decisively. We have to act quickly. And we can't just sit about and think, okay, what do I do now?

We have those plans in place.

We have all been working that. As you heard earlier, and one of the earlier panels, in 2016, July of 2016, our summer conference, we had almost zero discussions about cybersecurity.

In February of 2018, 75% was about cybersecurity.

Our summer meeting this past summer was about 75% again.

Cybersecurity is now on ... is our focus. And what keeps us up at night. Making sure that we have the right systems in place. That's where we have the partnership between the EAC, DHS, FBI, those partnerships are critical for us to defend our democracy, but to actually create a ... a system that is actually considered an election system with integrity.

And we just have to do our jobs.

And I think we're all focused on that now.

>> CHRISTY McCORMICK: Thank you. Thank you to all of you. I want to open this up to questions from the audience now.

We have somebody with a roving mike. Again, the rules are speak into the microphone. Please tell us your name and your affiliation. And please ask a question.

Mark, do you want to go ahead?

>> AUDIENCE MEMBER: Thank. Sam Garrett from the congressional resource service. I'm wondering, both the state and DHS side, what do you see in terms of states' abilities to make additional use of the resources you're providing? On the state side, spoke about funding, but do you feel like you have the technical expertise and the personnel that you needed and on the DHS side, do you feel like you have the elections expertise that you need to provide those

services? Thanks.

>> JIM CONDOS: We have to remember, we have 50 states and there's 50 different ways of doing business. You know, my state has 625,000 people. We have about 480,000 registered voters. That's a city block in New York City.

It's -- it's a different scale, but we all have our different situations. My IT manager happens to have come to us from the military. He was cybersecurity in the military. So he's got a good background.

But then you look at California, and they just set up a cybersecurity unit, if you want to call it that, with a $3 million cost. You know, it's apples and oranges, but we're all doing the same thing. And it really comes down to, every state as different procurement rules. At one point we were criticized because of the states were criticized because they hadn't spent the $380 million yet. We only received it in May and June, and if anyone knows anything about how state governments work with procurement, you know, to say that we would have even spent it by now is really pie in the sky stuff.

Anybody that actually -- I came out of the private sector and I think that the way we do business, the way I've been doing business on any IT solution, we do a business requirements, business analysis up front. We spend 8-12 months before we go out for an RFP for something. And we have situations, penetration testing, the vulnerability. We started back in 2013, so we were sort of ahead of the game, but we have done a lot of the work. We completed penetration tests not that long ago that showed we were a mature system, good defense build into it.

We are using the cyberhygiene scans that the DHS provides. We do that on a weekly basis. Going forward we will use them for some additional penetration testing. It's always a good idea to use a different set of eyes. And my view s for instance, we did a penetration test a couple of years ago and we just did one recently, two different companies. I wanted different companies because I wanted a different set of eyes looking at it.

And there's a lot of other things that DHS has rolled out for us, but many of us are doing it through private sector as well, but we'll utilize -- I know our state is going to utilize the DHS services. We're just not there yet.

>> CHRISTOPHER KREBS: I think the important thing to keep in mind for DHS. It's not our role to build the deep expertise -- that's what the state and local partners is for. We provide the unique technical security expertise to help complement, supplement, and boost as necessary our state and local partners. So we continue to look going forward to what are those unique capabilities that we can bring that the market's not already bringing or they don't have in house. And in part that's providing intelligence and the intelligence community and scaleable services like cyberhygiene scanning, like some of the configuration assessments, like some of the risk and vulnerability assessments.

>> AUDIENCE MEMBER: Hi. Dustin with Wall Street Journal. A question for Bill, just following up on comments about China. You

said we're not seeing the voting disruption that we saw in 2016 with Russia but we see some influence. You said China has interest in candidates that are pro-China. I want to clarify. Are you -- is the intelligence community seeing active efforts on social media disinformation efforts by China in -- to this specific election, this midterm election, and is it targeting certain candidates in a certain way that as you said, are pro-China?

>> WILLIAM EVANINA: The information to our China that is steady for years, it's nothing new but it's come to the forefront where we talk about it more and see the impact that we have. It's obviously the Russia attempt and the success we look at what they did with social media perspective in 2016 is a shiny object. But we are trying to promulgate that. And we see that influence attempt from China. With respect to actual ... affirmative efforts to impact voting machine or elect system, critical infrastructure, we haven't seen that yet nor have we actually seen intelligence that promulgates the will to do that. But it could just take one day, one effort, one thing. So we want to make sure that we don't just focus on Russia. China plays a part and they have an influence in the operation and they bank roll a lot of English speaking media activity here in the US that gets to the hearts and minds of people and potential voters. It's part of the process and we want to amplify on that.

>> CHRISTOPHER KREBS: While we haven't seen anything at the level of 16 or even near the level of '16, we don't need that. We're planning to a baseline of 2016 activity and then some. This is part of that, like, skating to where the puck is.

Yes, they demonstrated the capability in '10, the Russians in particular in 2016, but if we know anything about Russia, they get better. They're always getting better so we have to plan accordingly. When I engage and provide resources, we're not looking as if it's Russia, Iran, or whatever -- we are threat agnostic.

We're looking at building the baseline of security across the ecosystem up.

>> MAC WARNER: What a powerful panel. That is manifestation of the communications we started with. That being said, I'm going to rip the scab off and go back. And there is a question in here, and I'm going to be asking Bill to predict where we're going, but to lay the foundation, you all from the federal government perfect, knew something wag going on back when Jim just said, we were meeting the Secretaries of State in 2016, summer. You knew something was going on and come January of 2017, you designate the critical infrastructure over top of our objection and questions and so forth.

The federal government came in, weighed in and said it's going to happen.

So you all knew something but it wasn't being shared. We have much better communication going. Communication. And that is, right now, you've got four players. The people, the states, the federal government, and you have the capital markets represented by Facebook, Google, Twitter and so forth.

California went ahead for the people as a state and passed a privacy law and said we will dictate that capital markets playing inside of California and you're going to have to abide by our rules.

Those obviously don't want 50 different states passing the rules and the federal government is suing California. My question is, predict the future. Where is this going? Does the federal government know something and say dictate that or wait and hear the people or listen to the capital markets? Thank you.

>> So -- he saw looking at you, Bill.

[Laughter.]

>> CHRISTOPHER KREBS: I'll take a stab.

I'm just in general favor of smarter legislation, not more legislation. When we think about the long term, where this is going, Congress has been working in the policy makers and the policy thinkers have been working on just basic data breach legislation at a federal level for over a decade. Now we get into data protection, data privacy, that will add that complexity to the conversation.

And I've been working on name change, Bill, for my organization. I don't sound like a Soviet-era military intelligence agency. We're almost there! I promise!

[Laughter.]

We are weeks away from me never having to say that line every again, and I know the reporters in the room are happy about that.

But what can we do in the meantime to square the circle on those different players across the board, because it is very complicated to the 50 states all on the same page, some sort of alignment.

But what we are seeing, I think the capital market are responding.

2016 was a significant moment from cybersecurity perspective in that prior -- my sense at least, is prior to that, cybersecurity breach or an event had been IP theft a financial impact. This was really the first time that the American public realized that a cyber-enabled event could be, potentially, destabilizing of government. If not technically, then psychosocial. And that's an galvanizing moment, not just for the people, but for government.

The degree of coordination, cooperation across agencies is nothing I've ever seen and this is my second time in government. It's truly transformational.

The people, the companies, they are all on board. It is going to be, you know, quite a while, I think before we get a legislative fix but in the meantime we're starting to see an alignment of interests across the board.

>> WILLIAM EVANINA: I second what he said.

[Laughter.]

>> I think we have time for one more.

>> PAUL LUX: Paul Lux. If you Google Florida and cybersecurity, you're going to see the battle that ensued in Florida from about May until, you know, probably still ongoing, mostly, much of it attributable politically. But the glaring hole in the system that it has evidenced to me, those at the bottom end who actually have the responsibility to safe guard elections are not able to receive the actionable intelligence that you all are producing and that you all can share with certain people at certain levels of the state.

Do you support efforts to find some way of sharing classified --

whether you declassify it or dumb it down or whether you provide security clearances for those of us in the trenches, do you for that effort?

>> WILLIAM EVANINA: I support that we should not even have that discussion. I look at this as a threat-based initiative. If there is a threat posed to your county or you call yourself the lower level, that's a more linear perspective. If there's a threat -- whether it's through a phone call from Chris or a shop or a care line or any threat factor -- the FBI, victim notification, partnering with DHS, it doesn't matter. We have to look at this, not as an investigative product was because threat manifestation. How quick can we get it to the end universe? As quick as possible and real-time, just get it done. Worry about the consequences later.

>> CHRISTOPHER KREBS: Cybersecurity is an interesting space within national security because it's one of the few if not only areas of the domain where the private sector and the state and local governments are on the front lines. 2016, Illinois is in hand to hand combat with the Russians. We need to square the asymmetrical imbalance across the playing field and to do that, one of the things we can do, and we've committed to doing, share more information.

It took us a long, long time in 2016, even going into 2017, to ensure that everybody got the right level of information on what had happened in 2016.

In fact, it was last September when we finally got the square. Now, I'll add that the owner-operators are responsible parties of who owned the kit, the equipment, the network. They were notified. What we didn't have a full appreciation of at the time in 2016 was the complexity of the relationships of Secretaries of State, state election directors, state CIOs, homeland security directors, and we didn't have a good idea how the community interplayed. We've worked that problem and we have communications profiles now.

In the meantime, on the classification side there's been a lot of discussion about clearances and getting them out there. I think that's a distraction. We've talked about the trust piece. In meantime, if I have a piece of information that someone gives to me, I'm going to get it there one way or another. There's a duty to warn. We can do one time read-ins. We can do rapid declassifications. But I'm telling you, if the FBI knocks, open the door. Have a conversation. If my guys knock, if my team knocks, open the door. We don't -- you know, we don't just go knock on doors for fun. I think we're well, well past where we are in '16, but you know, the common refrain here is that this is not a sprint. It's a marathon and it's not even a normal marathon. This is an ultra and beyond.

>> CHRISTY McCORMICK: Please join me in thanking this auspicious panel. We appreciate this information.

[Applause.]

I want to invite up Chairman Hicks to close us out until this afternoon, when we will be visiting with the voting system vendors across the hall.

>> THOMAS HICKS: There we go. Another hand for the panel. Great.

[Applause.]

First, let me offer my sincere thanks to Senator Blunt and Klobuchar for visiting today. Their attendance, remarks, and support of the commission's work was invaluable.

All our moderators and panelists and others who spoke today well, appreciate your time and commitment to this very important mission, and EAC staff, I'm not naming you all but you know who you are. If you want to raise your hands and say, be acknowledged for the hard work that you did.

[Applause.]

As the chairman of the agency, it's not an easy person to get along with, and -- so -- and -- and to acknowledge you as the audience for coming here today.

I know that you're all busy, and -- but this is a very important matter that we wanted you to participate in.

And we're only halfway done through this.

So we're going to break for lunch at 1:00, and at 2:00 -- or 2:30, we're going to have some very special things going on.

One, the vendors are going to be in this room. So this room and the one immediately -- 45 degrees that way are going to have an open house and demonstrations of their equipment. And then for those of you who have asked questions about these various things, the EAC is putting on demonstrations, one on risk-limiting audits and other postelection audits. And EAC trainings and exercises which will be in 208 and 209.

And the testing and certification overview.

So I ask that you all come back at 2:30 to participate in that.

And again, I ask the President to give you a warning at 2:20 to let you know to come back here.

[Laughter.]

So that will be that.

And the other thing that I would like to talk about is, I invite you all to look at our website to learn more ways to help election officials administer, secure, and have accessible elections. Right now, the commission is in the midst of a year-long campaign, #countdown18, to promote resources for election officials and voters ahead of next month's election.

We ask that you provide us feedback, either to myself, positively, or negatively, to Vice Chair McCormick --

[Laughter.]

Wasn't meant to be said like that! Or EAC staff if you have ideas to help us do our mission better.

We will break until 2:30. This room will be flipped, so I ask that you don't lollygag. Just go. And come back at 2:30.

And lastly, we are extending the deadline for the Cleary awards. You've heard a lot of great innovations and ideas. We had Friday set as the deadline and we're going to extend it out to after the election and possibly to November 30th. But for those who have already submitted things, yours will be placed at the top of the list of being looked at.

So with that, I want to say thank you again, and I will see you at 2:30.

[Applause.]