United States Election Assistance Commission

Public Forum on Election Security in 2018: Perspective from State and Local Officials

Held on

Wednesday, April 18, 2018

at

Hyatt Regency Coral Gables

Coral Gables, Florida 33134

VERBATIM TRANSCRIPT

The following is the verbatim transcript of the United States Election Assistance Commission (EAC) Forum on Election Security in 2018: Perspectives from State and Local Officials that was held on Wednesday, April 18, 2018. The meeting convened at 2:03 p.m. and recessed at 4:13 p.m.

***

[Call to Order]

CHAIRMAN HICKS:

Let's start again. (Laughter) See I am so used to hearing my own self speak that I figure that everyone else can hear me. So, again, welcome to Miami. To all of you who are here in our studio audience and those of you on line, welcome to the forum that we are having today on US security. For those of you who are here, please look at your phones and silence them. Thank you.

I want to note the importance of having the opportunity to discuss election security and to hear directly from state and local election officials. I want to talk about a little bit and thank the Congress for the $380 million that they have appropriated for the purpose of increasing security and other factors, particularly the Rules Committee in the Senate and the House Administration Committee. The two committees with jurisdiction for the Election Assistance Commission.

Today is an opportunity for state and local election officials to offer their concerns and statements on election security. And I want to welcome you all here again today and then Commissioner McCormick, do you have a few words?

VICE-CHAIR MCCORMICK:

Thank you, Commissioner Hicks. I am Christy McCormick. I am vice chair of the EAC. I would like to ditto Chairman Hicks and welcome you all to our EAC forum on election security, and to those on line watching this afternoon, events like this are very important to us as EAC Commissioners and our staff as well because it helps us understand the issues facing election officials better, and it gives us information and perspective on how we can serve state and local election officials as they run our country's elections.

I would be remiss if I also did not acknowledge the Trump administration and those in Congress, especially those whose leadership helped to secure the $380 million in HAVA Funds for the states to improve the administration of elections prior to the 2018 election this year.

We are very thankful for Brian Newby, our Executive Director and for Dr. Mark Abbott, our EAC Grants Director, and our other staff members who have surpassed any other effort that I know of, of this type in getting these funds out to the states in record breaking time. Just weeks, which for the federal government is pretty amazing. I was able to call a number of the state officials to inform them of the amount of the appropriation that their states will be receiving and received the whole gamut of reactions to that

news, but I want to report that we are in really good hands with those who are responsible for conducting American elections.

Across the board we have serious dedicated public servants who place as a top priority well run, secure, and fair elections. The administration of elections has changed dramatically over the past eighteen years and are continuing to change, and we are in a completely different environment even in this past two years.

Election security is now in the forefront in the minds of all election officials across the country and I am looking forward to hearing from just a few of them and hearing their perspectives on the issue.

The EAC's mission is to serve our election officials, so I hope that the statements that they will give us today help us serve the election officials even better.

I am going to turn this over to our Executive Director Brian Newby at this point, but I also want to urge those election officials who are not able to be here today to let us know what your concerns are and what the EAC can do to help. Please reach out to me directly or to one of our staff, on line or on the phone and we will do whatever we can to assist you in this important effort.

So, thank you again for being here and I will introduce Brian Newby, the Executive Director of the Elections Assistance Commission. Brian?

MR. NEWBY:

Thank you, Commissioners. When we first came up with the idea of this forum, the thought process was that there were many people who have weighed in on the idea of election security and we wanted to have an opportunity for election officials expressly to speak about their thoughts about election security, so this was for elections officials, by election officials. That was really the concept behind the meeting.

We have created a number of resources on our website EAC.gov for security best practices. We conduct IT training for election administrators, we have also created a video that election administrators can show to civic groups, rotary clubs, that type of thing, to explain how election security works before they get in to the specifics of their jurisdiction.

I think we were all disappointed when we had the government shutdown leading to our cancellation, or at least postponement of the earlier meetings in January. But that process actually manifested itself in to the Omnibus Appropriations Act in March, which then included the $380 million in grants, or HAVA funds for many things, including election security. And it gave us the opportunity now, to be able to speak to that as part of this forum.

So that is what we are going to do now. In a moment I will hand it over to Mark Abbott who has done a terrific job getting ready, getting the money prepared to be distributed to the states. I want to show you just one quick map, you see, it just kind of gives you an idea of how the funds are spread out, the more green you see the more green the states get basically. And that is about the level of detail I am prepared to explain here right now.

So, I am going to now hand it over to Mark, who will get in to all of the details of the process.

***

[New Help America Vote Act (HAVA) Election Security Funds (Mark Abbott, Director of Grants, EAC)]

***

MR. ABBOTT:

Thank you, Chairman Hicks, Vice Chairman McCormick, I appreciate the opportunity to speak with you and our election officials across the county today about these grants.

The EAC team has done just a ton of work in the last three weeks to get to where we are today. And I am happy to give a very brief overview of the process for getting the money -- for putting together some plans on how you are going to use the money and talk some specifics about the way states might use those funds.

So just a quick history, so we want to talk just a little bit about what kind of money we have at the EAC over time. It's

actually been eight years since we have had money appropriated by Congress and the last money that we received was Section 251 requirements payments to meet the actual requirements of Title 3, so it is very specific purpose on those grants. Section 102 was to replace a type of equipment that Congress decided we should no longer use. So it was a mandate and there was money sent -- appropriated for that purpose, a long time ago, back in 2003.

Section 101 money, also in 2003, was to improve the administration of elections and it listed some things you could do with the money, but it was the most flexible type of money available to the states at the time. It really put the onus on them because they knew best what they needed in their state and allowed them to administer these funds to improve their federal election processes.

So, when it became apparent that we were going to get additional money for security and improvements to elections, we thought 101 was the place that the money might go, Congress agreed with the staff and were able to make the appropriation of $380 million, signed on March 22, under Section 101 of HAVA.

This money needs to be expended by 2023, so it's not here forever. We have 5 years to draw down and use the money. The award packets were issued on April 17, which I thought was a good day since mostly Uncle Sam was taking money from us, but we

were able to turn around and give a fair amount back to the states for elections.

The award packets has three parts to it. A Notice of Grant award which is a legal document that allows states to access the money and gives them the requirements they have to follow if they are going to take the money. And some instructions of how to draw the money from their accounts at the US Treasury and then somewhat uniquely, we have this 90-day deadline in there. And that 90 days is how long states have to put a plan together for how they want to spend that money.

These plans are one to three pages in length. We will post them on our website. We are going to offer some technical assistance and support as states begin putting these together. But they don't have to put the plan together to access their funds. The funds are available as of today. So you can go to our website, you can pull down a simple template to request your funds and you can have the money in three to five days in your account at your state to spend on any immediate needs that you know that you may have, in the run up to the 2018 election.

So even as you are spending money on things that are really important, you also have the 90 days to put together your plan. Congress was pretty specific when they said listen, this is what we want the money to go for. It's to improve the administration of

federal elections. Including enhanced technology and make election security improvements.

Election security is what is on everybody's mind. It is why we are here today. There has been a tremendous amount of press on this topic. And I am happy to say that the 101 funds are probably the best vehicle we have at the Elections Assistance Commission to allow states the flexibility and speed to put in place what they need.

So, you can improve it, administration generally. It is a very broad category, and, on the website, you will find all kinds of examples of how states have done that in the past and what the EAC has set as allowable there. You can do education, training, equipment, voting systems and technology as well as methods for casting and counting votes. You can work on accessibility, quality as for language accessibility, as well as handicap accessibility, the quality and quantity of your polling places.

There is a broad gambit of stuff here but if you look closely at what HAVA authorizes, you can see that some of the critical parts of what we need to do, and positioning for a more secure vote, and feeling like we have a more secure vote is around communication, training, convening, the kind of things that traditionally we just don't have funds to do at the state level. This money can be used for that.

We are getting lots of good ideas from states now on how they plan to use those funds. We will post those ideas on the website and share them as broadly as we can as innovative ideas roll in from our partners from the states.

So that is a very brief overview of the funds. I think the highlights are it's flexible money because we know states know what they need, and they have 90 days to talk to their stakeholders and figure out exactly how they want to deploy these resources over a five-year period of time. And the money is available now. Because we know the issues are now.

So that is it for my part and I can answer questions, and I will be available afterward.

One other thing, I also have with me Mike Kenefick, he is a contractor for the Election Assistance Commission, and he has been contracting with us since 2010. He knows HAVA very well and the funds well, he helps with our audit resolutions. He is available today and through Friday to answer questions and help states get ready to request the funds and begin spending them. Thank you.

CHAIRMAN HICKS:

Thank you, Dr. Abbott and Executive Director Newby for your comments here today. I have a few questions, most of which I do know the answers to, but it's more of making sure that those

folks who are out there in the audience and on line, who have these same questions get those answers. These are some of the things that I have been hearing for the last 40 days or so since the President signed this on March 23. When is the money available?

MR. ABBOTT:

So, the money is available as of yesterday, so, states simply have to follow a five step process to access the funds and we can have them in the state elections funds, the full amount available to your state or a portion of the amount available, it's the state's discretion how much they want to pull down and what time they want to pull it down, from the US Treasury, as long as they do it within five years.

CHAIRMAN HICKS:

And so, the 90-day period for states to issue their two to three-page narrative, when does that clock start?

MR. ABBOTT:

So that started yesterday. So, I think if I did that right it's July 15th or 16th that we are looking to have those back from the states.

CHAIRMAN HICKS:

And since this is 101 funds, Congress has said that they would like for states to use this money to purchase new voting equipment. They were explicit on what kind of equipment they

would like, but that still means that they have to adhere to the law in assuring that those who have disabilities can vote independently and privately. But that being said, there are very few restrictions on what this money can be used for. Correct?

MR. ABBOTT:

That's correct. There is, of course, Congress can choose to say we want you to do this and pass a law, very specifically like replacing punch card voting systems. They didn't do that in this case. They said we want you to work on security, we want you to look at these machines that perhaps don't have the audit trail that people are looking for, but the decision as to what you buy and when you buy it is yours at the state level. So that is how it was decided.

CHAIRMAN HICKS:

Director Newby?

MR NEWBY:

Well if I could just add, I think that our view is, two aspects. For one, we were going to judge our success in this in terms of the EAC, and how fast we get the funds out, and then how officially we can administer the program, and I think Mark has done a great job with that aspect.

The way the funds can be utilized sync with Section 101 of HAVA and that can include improving the administration of

elections which includes election security. And so, the key thing we want to say is that there are very few restrictions on the way these funds can be used, and Mark is an expert in knowing what those restrictions are.

CHAIRMAN HICKS:

All right. And so, I have already received a few comments, but the question from your first slide, being that it looked like the states of Montana and North Dakota were white in there, and basically was the same as the color of the Atlantic and Pacific Oceans, meaning that the Atlantic and Pacific are going to get zero. But each state will receive at least how much money?

MR. ABBOTT:

$3 million. That is set by a formula in HAVA that was modified in the appropriation this year to make sure that the small states received enough funds to do something with.

CHAIRMAN HICKS:

Thank you. Commissioner McCormick?

VICE-CHAIR MCCORMICK:

Yeah, I just want to clarify that the territories are not getting $3 million, right? They are just getting $600,000?

MR. ABBOTT:

The 50 states get the $3 million, is the minimum, for a small state minimum and then if you are a US territory, not Puerto Rico, the other territories you get $600,000 in federal funds.

VICE-CHAIR MCCORMICK:

But the territories don't have a match requirement. Is that correct?

MR. ABBOTT:

That is correct.

VICE-CHAIR MCCORMICK:

So, there is a five percent match. Could you give us the sort of outline of that five percent match?

MR. ABBOTT:

Right, so this was the other adjustment. The funds were adjusted in two ways in the appropriation. They were made one-year money, which means you have five years to spend this money rather than being available forever, or in perpetuity, like older HAVA funds were. And there is a match on this, and it's five percent of the federal share.

So, on the chart that we posted on the website, you can see what your match obligation is, but you do not need that match obligation up front. You need to produce that match over a period of two years. So, we will look for that documentation on your federal financial report that the states submit to us annually.

The match can be cash or in kind. In this case, an in-kind contribution would be something else you are purchasing or doing with non-federal money that is in line with what you are doing in your grant that can count as your match. So, the match can cascade down to the local level. So, we know every locality is working on security as well. They may well easily have the five percent they would need if the state chooses to put some of the money they received down to the local level to be spent there.

VICE-CHAIR MCCORMICK:

And if they have already spent the money in this fiscal year, can they use that as a match prior to this bill being signed?

MR. ABBOTT:

So, there is a question of when the grant actually starts when the President signed the bill. The omnibus appropriation goes back to the beginning of the fiscal year, so the state should contact my office if they want to have costs that were incurred after October 1, 2017, included as match or as part of the federal share. We will work through those and adjust their awards as needed.

VICE-CHAIR MCCORMICK:

Make sure they'll pass audits. Right?

MR. ABBOTT:

That is correct.

VICE-CHAIR MCCORMICK:

Yeah.

MR. ABBOTT:

I didn't mention the audit obligations here. It's been a long time since we've had new money but there are serious audit obligations the states will face in accepting these funds.

Our office, the grants office, our job is to minimize those risks and provide the right kind of support and technical assistance both before and after the audit to make sure that states can be focused on using the money for the things that they need to get done. Not worrying necessarily about the audit situation for them, so we will make sure they are well educated and have the material they need to be successful.

VICE-CHAIR MCCORMICK:

And that the narrative really goes to that audit situation, right? That's documentation so that, they have some sort of documentation to show when they get audited that they are appropriately using the money.

MR ABBOTT:

That is right. We need an audit standard. The standard is found in OMB circulars that tells you what kinds of things you can do and not do with federal money. What kind of record keeping you need to keep, for example.

The three-page narrative in the corresponding budget allows us a guide to audit against. So, if you do these activities, and you say you are going to do these activities in your plan and your budget reflects that, and then you do entirely different activities that's not in your budget reflects something -- that's not reflected in your activities, that will be questioned in an audit.

So those standards, you are setting your standards for how you want to spend the money and the auditors will audit against what you said you want to do.

VICE-CHAIR MCCORMICK:

Can they update or amend those narrative statements?

MR ABBOTT:

Yes, as needed. And I fully anticipate doing rounds of revisions. After you hold an election you see things you didn't see before. You may want to deploy these federal resources against those needs, that is absolutely allowable and encouraged.

VICE-CHAIR MCCORMICK:

Now I know Congress wanted this money specifically to be used as soon as possible and that is why they made it pretty much no strings attached and wanted to be flexible and get this money out.

If the states draw down the money within the five years and hopefully spend it, but if they don't spend it can they hold on to that money or do they have to actually spend it within the five years.

MR. ABBOTT:

So, we have set a five-year project period for these funds so the EAC's grants office expectation is that you are going to use the money over a five-year period. If you need the money over a longer period of time, then we can look at doing an extension for that program period.

I think that, unlike the early money, which some states used as a rainy day fund or for emergencies or contingencies that they weren't aware of yet, which was a very fine use of the money and allowable under the law. We don't have that same flexibility this year. If congress wanted to give us that flexibility, they could have in the appropriation. They did not. So, we are putting everyone on this five-year clock, and we want to help them get through this trough of money in five years.

VICE-CHAIR MCCORMICK:

Yea, thank you for that because I did have some questions when I called the states, kind of in that vein. You know, how long they had to spend the money. Whether they could hold it for a rainy day fund. Things like that.

So, I appreciate that clarity and would urge the states to work with Mark and work with our staff to make sure that the way the money is going to be spent will be appropriate and they will be able to pass the audits, the required audits that the federal government requires. So, thank you for that.

CHAIRMAN HICKS:

I want to thank you both but before we leave, before you leave the panel, the EAC will be holding several conference calls and webinars over the next few months for states to ask questions and go forward with this as well. Correct?

MR. ABBOTT:

That's correct. So that will be on the website. We will post to those and we will do as many as we can, so that as we learn new things from our partners in the states we will make sure that gets shared.

MR NEWBY:

And if I could one thing we would like to do going forward as this program starts to get implemented is highlight the successes that states and localities have by using these grants, and create a series for a clearinghouse that explains and promotes the uses that some users have for this money.

CHAIRMAN HICKS:

Okay, thank you.

VICE-CHAIRMAN MCCORMICK

Thanks very much.

***

[Election Cybersecurity Update from the Perspective of Local Election Officials]

***

CHAIRMAN HICKS:

So, know we are going to have the local election officials come up to the table and after that we are going to have the state election officials do their panel. The third panel will be an open mic. And that open mic is for election officials only. So, we're looking to hear from election officials who are here today on the process they are doing in terms of security.

And as these folks get situated, I want to make you aware of a clock that we have up here. Because, myself included, I like to talk on and on and on, but we don't want to go all night. So, the clock is going be set for each of you for five minutes. The green light is your time, yeah David I am looking at you. The green light will be for four minutes and 30 seconds, and then it will blink yellow for 30 seconds. And then the red will be a please stop, please wrap up, and I believe it will actually make a noise. (Laughter)

So, that being said, I want to introduce our panel here today. Starting on my left. Lance Gough is the Executive Director, Board of Elections Commissioner for Chicago, Illinois. Lance has been

the Executive Director, managing voter registration, election administration for 1.5 million voters for three decades.

During his tenure the agency has been a pioneer on several fronts, including the recruitment and training of 2,000 high school poll workers in every city wide election. Being the first major jurisdiction to utilize electronic poll books in every precinct and lobbying successfully for on line voter registration. Election day registration and on-line ballot access for military and overseas. Lance, thank you for being here today. I look forward to hearing your feedback.

I can introduce all of you or just, let me just go down the line. Ricky Hatch, who is the Clerk for Weber County, Utah. Ricky was elected Clerk Auditor for Weber County, Utah in 2010. Ricky was honored by his fellow County Auditors as Utah's 2013 Auditor of the year. In 2015, clerk of the year. Ricky has previously served as Information Systems Auditor and consulted for Price Waterhouse. A Business Analyst and Project Manager for Parametric Technology Corporation, and as a Financial Analyst for Jetway. Thank you, Ricky, for being here today as well.

Noah Praetz, Director of Elections for Cook County Clerk Office, Chicago, Illinois, which is different than the Board of Elections for Chicago. Noah serves as Director of Elections in Cook County, one of the largest jurisdictions in the country.

Each year his team services 1.5 million voters and facilitates democracy for thousands of candidates and trains and supports thousands of volunteers to administer democracy. He started as a temporary worker hired to help during data entry to the 2000 Presidential Election.

He worked his way through the ranks, doing nearly every election job in the department. Learning the pain points and opportunities while going to law school at night. Noah became Deputy Director of Elections in 2007 and was appointed Director in 2013.

He is a board member of (IAGO) International Associations of Government Officials, along with Ricky as well. He also serves as the elections center and Illinois Association of County Clerks and Recorders. He has presented on stability, election day management, on line registration, voter registration modernization and other election related issues. And today he will deliver his remarks on election security.

Last but not least. David Stafford is the Supervisor of Elections for -- I always pronounce it wrong, so I'm going to let you do it -- it's Gambia County, Florida, which is up in the panhandle.

David was elected in 2004, in addition to his work in Florida he also serves in leadership positions to guide election policy at a national level, including co-chair for CSG Overseas Voting Initiative

Policy working group and is a Board Member of the National Advisory Board Elections Systems and Software, and as a member of the technology and elections working group for the US Elections Assistance Commission. He previously served as the northwest Florida Director for US Senator Connie Mack, Chief of Staff for US Congressman Joe Scarborough, Producer for MSNBC Cable News Network, and Director for Federal Affairs at Grocery Manufacturers of America.

I want to thank you all for being here today and Lance we can start with you.

MR. GOUGH:

Thank you, thank you for the opportunity to testify in front of the Elections Assistance Commission. To both commissioners, it is a pleasure to see you again. Those of us with decades of experience in election administration have weathered many changes. Introducing of new voter equipment under HAVA. Introducing of election early voting. Expanding the use of vote by mail. In some jurisdictions electronic poll books. And in jurisdictions like mine, on line registration, election day registrations and automatic registration.

Clearly the newest challenges need to be maintained the faith in the security of our election franchise. One of the first episodes that brought about this change was the Russians hacking

in to my home state, the state of Illinois, state board of elections voter registration data base. To me this was just as significant as the problems we experienced with punch card voting. After hacking in the summer of 2006 affected no individual's voter registration records. I would like to repeat; the hacking had no effect on no individual voting records. It had no effect on balloting systems.

The Illinois registration system is merely a gathering, a reflection of 109 counties that feed their data in to it, so none of those were hacked at the time. Which brought a problem that we had, the Russians, managed to do something that really caused a major problem. They undermined the faith in our franchise.

Similarly, in Chicago, we had exposed in the summer of 2017. I received a call on Saturday. In fact, the person that called me is sitting down from me, Noah Praetz, called me up and said, Lance, looks like something happened. Your voter data is out there, because he got a call from the FBI.

We found out that it was from a vendor that was working on electronic poll books. After we found that out, we were able to shut that down. We had the information, we went through the dark web. Found out that none of this data got out. In fact, the only person that saw this data was a security cop that gave the alarm and told us what was going on.

As soon as we found that out we then contacted the media. I contacted election officials around the United States explaining what happened. I contacted law enforcement. We went right down. We had a press conference the next day. Spoke to the media, explained what happened, that no data got out.

But because of that has left us wide open. What we need to do is concentrate more on who has our data. And this was a vendor that has been in the election field for many years. And after that has happened we had to rethink what we need to do about our data.

Our data needs to be controlled in case somebody could hack into it, it can't do any good. We want to reduce the amount of data that is out there on the web. I know we have to have person's name and address, but we don't have to have their full birthdates, we don't have to have their last four digits of social security.

So, what we are doing is we are going to scale back on any data that's going out. So, in case if somebody ever did get in to the system, which I am hoping it will never happen again, but who knows.

With what is going on right now, we have word that we see that people are hacking in to people's home computers now. Routers are being hacked in to. This is something that we need to really take a look at. So, I just want to say that we are going to

reduce the number of stuff that is out there. We are going over security procedures with all of our vendors. Our website managers, our web farms, even our printers that print out our verification of registration cards, all of that data is going to be reduced to bare bones. Hoping that if we do get hacked again, which with the way things are going who knows what will happen, that we will be prepared, and nothing will get out.

So, thank you for letting me speak. We are looking at least risk management. We are looking at the least problems and get that information out there.

CHAIRMAN HICKS:

So, I did notice that, thank you for your testimony and I do have a few questions, but I think that it would probably be best if we let everyone speak and then do a round of questions that way.

MR. GOUGH:

Very good.

CHAIRMAN HICKS:

The timer itself is going to be, it blinks at two minutes and then at one minute it starts doing the yellow blink beep. So, Ricky whenever you are ready.

MR. HATCH:

Thank you. Thanks for having us here and having this event.

The biggest cyber security hurdle that we face as election officials isn't a piece of technology, it isn't even a thing we can purchase and install. It is building and maintaining public trust. In life, most stuff flows downhill. Water, mud, rocks. And when things go bad in an organization other stuff flows downhill. And it gets worse the farther down it goes, we have all seen it. But when it comes to trust in government, gravity changes course. Trust flows uphill. Let me explain.

There are a couple of polls, one from Gallup, one from ugov that shows that 71 percent of Americans trust their local government to handle problems, while only 62 percent of them trust their state government. And the number drops to a dismal 31 percent for the federal government. Trust starts locally and flows up the mountain.

It is the same with public trust in elections. The closer the election is to home the more likely we are to trust it. Why? Because there is a name and a face. Because I as a voter can observe the process, ask questions and actually talk to a human being in my own county. Not someone further up the mountain at the state capital or back in Washington, D.C.

A voter's trust in the nation's elections process is driven by the voter's experience with their local election office. Whether it is registering to vote, receiving a ballot in the mail, using voting

equipment at a polling place, or checking out election results on the web, the voter's interaction is almost always with their local election official. Local election officials are the face and the voice of our nations elections infrastructure, and they are what drive the fundamental level of trust in every single election.

This is how it should be, but it does present a challenge. The very level of government that the voters trust the most to secure their elections is also the level that has the fewest resources to do that, and has the least amount of control over how these new federal funds will be spent.

In fact, as I have studied federal legislation and participated in cyber securities over the past couple of years, it feels to me that when state and federal level folks use the phrase state and local election officials they often mean state election officials. I don't think this is intentional, I think it is just a mind set that needs to be examined.

Now I realize that I sound like I am griping. Like I am saying that local election officials, like Rodney Dangerfield, get no respect. Right? And I don't mean to, but we need to recognize that local officials need to be the face of elections to the country because they are the ones whom the people trust. And they need the money and the training to do it right.

There are almost 9,000 dedicated local election officials throughout the country and the vast majority of them are small, underfunded and not staffed with cyber security experts. Over 2/3 of them have fewer than 20,000 voters. Only 300 of them, or about 3 percent, have joined the election infrastructure ISAC, or Information Sharing and Analysis Center. I'll bet about ¾ of them haven't even heard about the EI ISAC yet.

Now our challenge as federal, state and local election officials is to figure out how to support the local officials with the training, technology and funding so they can insure their own house is in order and then confidently educate the voters about the security of their elections. One way to do this is to ensure that when these federal HAVA funds start flowing downhill that they don't all stop at the state level.

Now of course, most states are the keepers of the voter registration data bases, which are critical to the integrity of the election. They absolutely need funding to ensure that these voter rolls are secure, but the funds must not get stuck there. They are needed at all levels, especially at the level that voters interact with the most.

These funds, when accompanied with training and expertise from our state and federal partners, they will help local election officials properly implement cyber security tools and educate the

public to ensure that public trust in the election's process stays strong.

Fortunately, the EAC and DHS have already been working with state and local election officials and organizations like IGO are pitching as well. In fact, IGO has a webinar tomorrow afternoon to show officials how to use some specific, free private sector resources to stop D DOS attacks.

Now we appreciate being involved from the beginning and we commit to bring our A game with us as we work together, federal, state and local election officials, to strengthen the public's trust in our nation's election infrastructure. Thank you.

CHAIRMAN HICKS:

Thank you, Ricky. Noah?

MR. PRAETZ:

Okay. Well, thank you commissioners. Our elections were attacked. The national security community warns us to expect more sophisticated and evolving attacks. Make no mistake, local election officials are on the front lines, 108 in Illinois and over 8,000 nationally.

Most of us are county officers facing down powerful, shadowy adversaries like county sheriffs sent to repel an invading army. Now many locals in the election community are pressing for resources. First, for better technology and routine hand counted

audits to get confidence that digital results are accurate. And second, and more critically today, we are pressing for top notch personnel with skills to navigate the cyber mine field.

Our country's local election officials need direct human support as we work to defend ourselves against the onslaught of digital threats we have been warned about. Over the past 15 years our office has tried to lead on technology and security using applied forensics in elections, creating widely circulated cyber security checklists in advance of the 2016 elections. Publishing the first white paper written by election officials in the wake of the 2016 attacks.

Additionally, we worked with the Center for Internet Security and the Defending Digital Democracy Program at Harvard's Belfer Center to help adapt their digital security expertise to the unique context of elections.

As co-chair of the government security council that Homeland Security created to help address this election security effort, I have worked intimately with federal, state and local leaders in elections technology, intelligence and law enforcement. In all of these efforts, it became crystal clear that local election officials need someone, some person, to take ownership of security in each election office.

In our office we work with our colleagues, and my good friend Lance, at the Chicago Board of Elections to share the cost of hiring a digital security expert. I simply can't fathom how other election officials can meet a foreign threat without a similar support or a similar investment. And it's a hefty investment, but defense of digital systems is very difficult. Just ask Uber or Equifax. HBO or Sony. Boston or Baltimore. The EAC or OPM.

Congress just released $380 million to combat the election cyber security threat, and that is a very important start. It may be necessary to invest that much annually.

Meanwhile, Americans justly concerned about the cost need confidence this money will be well spent. In my mind there are two priorities. First, a handful of states and counties still have paperless voting systems, and these should be replaced as soon as possible. But second, everywhere, across the country, we must improve the defensive capacities of local election offices. Most are run by just a handful of incredibly dedicated and hardworking heroes, but just a handful of heroes making critical security decisions are out matched against the threats we have been warned of.

Therefore, I envision an army of digital defenders serving election offices around Illinois and the nation, starting now and

working through the 2020 presidential election at least. These digital defenders need to accomplish three vital goals.

First, they will improve defenses within election offices, following the specific recommendations of the Center for Internet Security or Defending Digital Democracy. Bringing up the floor of the election security ecosystem. Appropriately supported, we can see massive movement very quickly. There is lots of low hanging fruit.

Second, the digital defenders will work with outside vendors who provide much of the elections infrastructure, to eliminate or defend specific vulnerabilities. They will also work through the necessary work to secure the free support being offered by public and private organizations like Homeland Security or Google or Cloud Flare, or the Elections Information Sharing and Analyses Center.

And third, they will build a culture of security that adapts to the evolving threats we face.

This massive reinforcement effort can be accomplished, and it can be done now. It will require the states to cut through the red tape that can delay action. This may mean relying on existing contracts or even emergency procurements, but states must do whatever they need to do to get an army of digital defenders on the ground this summer. After all the danger is not hypothetical. We

are bracing against the renewed attacks we have been told to expect. If we fail to get experts in the local offices who will help the locals shore up our defenses, we will regret it.

Election officials deploy a variety of network connected digital services, such as informational websites, poll books, voter registration systems, unofficial election results displays. Each of these are ripe targets for our adversaries. A successful attack against those services may not change a single vote but it could still damage public confidence.

This is particularly true in a time of great suspicion. Disappointing gracelessness and highly partisan grandstanding. Losing candidates are already apt to call their defeats into doubt. A new digital breach, no matter how far removed from the vote counting system could turn sore losers to cynicism, disbelief, even revolt. That is the reaction our enemies want. We can't eliminate every chance of breach, but we can make successful attacks rare.

We secure ourselves best against the expected threat by investing in people first. Digital defenders who can guide a coherent flexible strategy against slippery adversaries. Thank you.

CHAIRMAN HICKS:

Last but not least, David.

MR. STAFFORD:

I feel like I should welcome you all to Florida, although I am closer to Dallas, Nashville, and Charlotte, North Carolina than I am to Miami, but welcome to Florida. Glad you are here. You are no strangers to the state. I appreciate your efforts over the years in supporting what we do down here.

I want to talk a little bit about what is going on with the Government Coordinating Council and the work with the Department of Homeland Security with our state and local partners, and then talk a little bit about what we are doing here in Florida.

The GCC, or the Government Coordinating Counsel, is making what I believe is great progress although the public generally may not be hearing a lot about it. When you look at the date of the announcement by Secretary Johnson declaring elections as critical infrastructure, it was only nine months later that the GCC was formed. Which, in federal government terms is lighting speed, in my humble opinion.

The sector coordinating counsel was formed shortly there after, and we immediately got to work. I happen to serve, along with my two colleagues here to my right, Noah and Ricky, on the government coordinating counsel, and we began to get to work very quickly. There was a working group established and we are coming up with a communications protocol. Very very important, I believe, in the work between the federal, state and local partners in

establishing some framework for how this type of information is shared, both up the chain and down the chain.

In addition, there was a pilot that was established in testing basically the multi-state ISAC for use for the elections infrastructure, and there was a decision made, that the pilot was successful so now we have established the EII SAC, and I don't want to steal Amy Cohen's thunder from NASED, but as of information I received today, 47 states, 2 territories, 376 local election offices and 3 associations are now members of the EII SAC, and I am proud to say that Florida's 55 out of Florida's 67 counties are members.

So, lots of great work is going on there, and generally I think the relationship between the Department of Homeland Security and state and local election officials has improved. There was great, I don't want to call it suspicion, but great unease initially with the designation because I don't think either side knew exactly what it meant. As the time has gone on and the officials began to work together with each other, I think there was a level of trust that is building and continues to build. We are not fully there yet, but I think that the partnership is working well.

The GCC also, I think, importantly, had ample representation of local election officials, kind of talking about what Ricky talked about earlier, when you hear state and local, a lot of times it's just

state. But there is a significant presence of local elections officials who are on the front line, which I believe is very important. And again, in that communications piece it is something that sounds really easy, yeah, of course we should be sharing information, but once you start scratching beneath the surface, how does that framework look like? What is an incident that meets the threshold of being able to be, that requiring to be shared and how does that mechanism actually work? It's a little more complicated than that.

But great progress is being made, led by Ricky. Ricky is one of the chairs of that working group, as well as the sector specific plan, which Noah is working on, which is basically the framework of what exactly the elections infrastructure sector is going to do.

It is wonderful that Congress appropriated that money, and it is even better that the money is going to be getting out quickly. Congress has also been involved in proposing legislation. And just one word of caution there, in my opinion, when you start getting too specific in statutory language, for instance the audit provision that was in one of the main pieces of legislation that is being proposed would require, I did a little analysis, 22 percent of my ballots in the 2016 primary election being subject to audit. That is a pretty high standard. I don't know, is that the gold standard? I don't know but I

would hate for that level of specificity be enshrined in statutory language.

Let me talk a little bit now about what we are doing here in the state of Florida. We understand the role that we play in national elections obviously. The legislature satisfied the Secretary of State's budget request for $2 million for counties to acquire network monitoring devices.

The supervisors themselves, the supervisors of elections have held two EAC sponsored IT training sessions. We devoted an entire day at our last conference to cyber with officials from DHS, FBI, FDLE, the National Guard and others there present.

So, we also are taking advantage of a lot of the resources that are out there from the aforementioned CIS playbook, the Defending Digital Democracy playbook, as well as other efforts like Cloudflare, Project Thenian, and Google's Project Shield.

So, we understand that we are on the front lines. We are working very extremely hard at shoring ourselves up and look forward to continuing the work with our state and federal partners to ensure that we are in the best position that we can be for the 2018 elections and beyond. Thank you.

CHAIRMAN HICKS:

Thank you, David. I have a few questions, but before I get into the questions I wanted to say, thank you all for serving as local

election officials. A couple of weeks ago I had the honor to go to a dear friend of mine's memorial Wendy Noren, who was a monster in terms of her tenacity and spirit, and if there were any awards given to local election officials she would have won it multiple times.

So, I wanted to thank you all for being a part of that because I know it is sometimes thankless, and sometimes it doesn't pay well, and so forth. But I know that I have confidence in the process because of the four of you being here and that work that you do.

So, with that I have just a few questions and starting with Ricky. David had mentioned what is the gold standard in terms of audit numbers and he mentioned 22 percent. What's a typical number that is used for audits overall?

MR. HATCH:

Before I became an election official I was a Financial Auditor and an Information Systems Auditor, and the standards are a little bit different there. Generally, in the world of financial auditing, if you have a sample size of 60 items to select, that provides sufficient coverage, assuming it's a statistical sample.

I don't pretend to say that that would be adequate in the elections world. We need to hold ourselves to a higher standard. In the state of Utah, we look at about five percent as the threshold that we look at and conduct audits on, and those are statistically

selected at the state level and then communicated down to the counties.

CHAIRMAN HICKS:

A couple of you mentioned Belfer Center, and Google, Cloudflare, and a couple of other things. I know that Microsoft is now doing something in terms of defending digital something or other, but they are now getting in that space as well.

Are there other companies that you know of, or institutions, that are doing things in this realm that could aid local jurisdictions? Excuse me, I say that because I know that it's not you, Lance and Noah, you come from a large jurisdiction, 1.5 million voters and so forth, and most counties don't have that number of voters, but they also don't have that number of election officials. So, the EAC has put together a program where one of the former commissioners would go out and talk to election officials, it's basically IT management for election officials. Giving them a basis for what they need to look out for moving forward with this.

Some of this can be found on our website at EAC.gov but I am hoping that we can continually build on that, because, as you know, elections are going to continue to happen. We have 2018 coming up. 2020 is right around the corner. This $380 million is a nice payment. I don't know if Congress is going to come back and give more money, but elections continue to happen.

So, can you talk a little bit about some of the other aspects that are out there, if any of you know, and what sort of role can poll workers play in terms of election security.

MR. STAFFORD:

Generally, what I have found is that I have yet to find somebody that's told me no when I picked up the phone and asked them to help. I'll give you a for instance. We happen to have the University of West Florida in my county and they've got a Center for Cyber Security there that's a recognized regional center and it was just one of those things, hey, this is now becoming an important issue, so I just picked up the phone and just called the head, the director of that center, and that resulted in a pilot program that was done at the state level with a handful of my colleagues and staff, who went through a really in depth training session there, to see if this is something that can be modeled or modified to work with state officials, local officials around the state.

So, there is a lot of resources out there. Just going out and asking people, because one of the things that everybody has pride and understands the importance of elections in the United States. So, when you call and ask them, hey I would like your help, I would like some advice, again, my experience has been people are readily willing to help.

Now some people may want to get, you may have to pay for some of these services, and whatnot. But generally, there has been a willingness out there for everybody to pitch in and say, yes, it is important that we secure our elections, and let us help you.

MR. HATCH:

The Department of Homeland Security has a ton of resources they've pledged and offered to help. Now, some of those are, it's going to take some time to get them deployed and out. So, there will probably be a waiting list for some of the services that are more robust, but they've given every indication that those services are available to election jurisdictions large and small,l which is great.

MR. GOUGH:

One of the problems is, let's take Illinois, for example, we have 109 different election officials that run elections in Illinois. Some have about 20,000 registered voters, some have less. They run their elections off of -- one jurisdiction runs their election off of all state's computers. What we need to do is get the word out to everybody, and you'll see that a lot of the associations like election center and other organizations are going to see more and more people coming to them to get information and help. And it's something that we need to get down to the smallest jurisdictions, because those are the ones that are going to be attacked.

MR. PRAETZ:

Yeah, I'll just echo, this is a weak link problem and they will keep shaking windows until one of them opens. Right? And it could be one of us up here or it could be the smallest county in the state. And the truth of the matter is none of the organizations right now have full blanket coverage or information sharing to every local election official. I think we recognize that in the Government Coordinating Council, one of our, we have three primary goals, one of which is to create a communication channel that gets to all 8800.

Two major problems. One is getting the information to people, but even with it, without extra dedicated resource committed to securing the office there's simply not the capacity.

I'm amazed every time that I meet with my colleagues from around Illinois how much knowledge they hold in their head. In a big office we're able to segment, create different silos of expertise, we've got the ability or capacity to pull on threads when we're interested in something like cybersecurity. That flexibility just does not exist.

I firmly believe this challenge is only answered with direct human resource placed in local election official's offices, people who have the capacity to accept a threat and then to work through all the free resources that are already there.

CHAIRMAN HICKS:

Commissioner McCormick?

VICE-CHAIR MCCORMICK:

Thank you to all of you for being here and I want to echo Chairman Hicks on thanking you for your service as a local election official. So, this is a tough job, and very complex and y'all have done an amazing job in your jurisdictions, and so I want to thank you again for doing a thankless job.

I think there's a silver lining in what happened in 2016, and that is we're focusing now on these problems. I know that election officials have always focused on these problems and to some degree, not so laserly focused on election security, but I think this has brought this to the forefront for us in the last couple of years. So, if there's a good consequence to what happened, that is one of them.

I think we need to understand our threat before we can address it. And so, I would like to ask, I guess, Lance, and any of you can join on, what could actually happen if someone gets into the system?

MR. GOUGH:

Depends on what kind of system you're talking about. Like voter registration system is, let's say if somebody got in and wanted to shut down our electronic poll books. Well, luckily, we have a

backup signature book that we have that will be able to get out to the precincts.

You know, we go back to paper. If electronic systems get hacked, we have to go back to paper based systems, and we're able to do that luckily. What I'm, what people are talking about is actually get in and hack the actual vote counting. That's very hard to do considering we have so many different pieces of equipment out there, and you would have to attack every single one that's not tied up to the internet or not online, which I feel that the ballot counting is secure.

It's the election database that was vulnerable. And that's one we need to have plans that we have to shut down and go back to another way of doing it. And that's paper. And it's always been a backup. Like we're going back to paper ballots right now.

If you remember in the beginning years, what we did is we had paper ballots. They went, you know, the poll workers with the more and more units of government, the ballots got larger and larger and it was harder to count. That's when we went to having equipment count the ballots in the precinct. Now we're looking at going back to paper ballots.

So, something that we need to actually look at and figure the best way of securing everything, not only our vote counting but also our actual infrastructure on who's voting and how we vote.

VICE-CHAIR MCCORMICK:

So, we've heard that the systems aren't connected to the internet.

MR. GOUGH:

They are not.

VICE-CHAIR MCCORMICK:

And, you know so we've got voter registration systems and then we've got actual voting systems, then we have tabulation systems, election night reporting systems. . .

MR. GOUGH:

Uh-huh.

VICE-CHAIR MCCORMICK:

Do we look at those all separately or do we look at them as a whole? David, what's your thought on that? Do we look at it as one single system?

MR. STAFFORD:

I don't think we look at it, I mean I think we talk about election systems and I think it's important verbiage that we are talking about here. Voting systems and election systems are not the same thing. And I think too often when people talk about things happening to voting systems what they really mean is election systems.

One of the challenges that overrides what we all do is the balance of accessibility and security. I don't think that's ever been in more focus than it is right now. For instance, it's easy for a private sector company to say don't ever open an email with an attachment that you're not absolutely sure what it is. Well, if you're in a public office and you're dealing with the public, sometimes they're going to send you an email, please see attachment. Okay?

So, it's not it's not as easy for a public agency sometimes to be able to have the same level of standards, I guess, as you wil,l as you would in a private sector. The other, I think, thing that the greater realization, I think Lance touched on this earlier, is that we've always been focused on security. And the main focus has been on what I will call traditional election security, your polling place security, your ballot security, the security of your voting equipment.

VICE-CHAIR MCCORMICK:

So, physical security

MR. STAFFORD:

Physical security, correct. Now I think there was, some were more focused on it than others, but now there's a realization and I think a level of urgency among local election officials across the country that this is an area where we need to spend a lot, and I don't think it's unique to elections. I think it's government wide and I

think it's private sector wide, that this is an emerging threat and we need to do what we can to meet that threat.

So again, verbiage is really important, when we're talking about things like voting systems and election systems. Because, you know, let's be clear, somebody somewhere in the state of Florida, in the state of Illinois, is going to go to their polling place on election day in 2016 and they're not going to be in the precinct register. They're going to go to a polling place in a primary election and their party affiliation is not going to be what they think it is or should be. How do I know it is going to happen? Because it happens in every election, and that in and of itself does not mean that election has been hacked.

So, I think we all have a level of responsibility to be very careful in the words that we use, and what's attributed as a hacked election versus what are the normal ebbs and flows of an election cycle. I don't know if I answered your question,

VICE-CHAIR MCCORMICK:

Even the word hacking is, you know, prone to misuse. What is a hack? Is it an attempt at penetrating a system? Is it actually getting into the system? I mean, we do have to be careful about our verbiage, and maybe we need to train some officials on that. That does affect voter confidence as well.

MR. STAFFORD:

Sure. And again, I think to just reemphasize, there is a level of awareness and focus on that cybersecurity side that there wasn't, there hasn't been to that level previously.

VICE-CHAIR MCCORMICK:

Ricky, you're working on the communication part with the Government Coordinating Council, I understand. What are some of the challenges in communicating the risks and threats right now?

MR. HATCH:

That's a great question. I hope we have several hours to . . .

VICE-CHAIRMAN MCCORMICK:

I understand.

MR. HATCH:

The idea is you want to foster as much communication as possible, but you also have to respect the different positions and levels that are involved in that communication. And some of the complications that occur when you have completely different entities that are sometimes forced together that may not even trust each other, or may have doubts about the other's motives.

Generally, in the elections world we get along so well at federal, state and local levels, we work closely, but it's not always the case. The first thing we have to figure out is what generates the sharing of information? What necessitates that? There's

always just general information sharing, but then you have potential incidents.

If we shared every time somebody had a DDoS attack, our inboxes would be overflowing all the time because that happens all the time, so that's not worth sharing. But where is the line and with whom do you share it? If my county comes under attack, should Noah know that? Well, probably depends on the severity and the scope, and possibly even the source. Should my state elections director know that? Probably. How about if the state is hacked. Should the local election officials be notified? I use hacked. Sorry. If the state is potentially breached or penetrated.

Those are some of the challenges that we figure out. At what point do, if my system has been breached at what point do I become a victim and then, all of a sudden you have the whole legal realm that you have to deal with, and the restrictions on being able to share information when there's a victim and a crime that occurs.

Those are some of the complexities with the communications document. I think we've got a great draft document in place. I expect it to come out, I'm hoping fairly soon. The GCC has had a first look at it. The DHS has looked at it. And I think the document will be very -- it has to be somewhat general, but it has a sufficient specificity without forcing, because it can't be

an enforcement document. But I think state and local election officials as well as DHS and EAC will find it to be helpful.

VICE-CHAIR MCCORMICK:

And this information has to flow back and forth up and down, right?

MR. HATCH:

Exactly, and sometimes across state to state or across counties.

VICE-CHAIR MCCORMICK:

Okay. Noah, you talked about not having enough resources. What can local officials do now even without having adequate resources?

MR. PRAETZ:

Sure. And I mean, I'm not complaining about Cook County's resources. Certainly, a play we could have made was to say, hey funnel all that money down by a count of registered voters, and Lance and I would take merely half of Illinois'' money, but what the ecosystem right now needs is a more equalized or distributed model.

You know, in Illinois each of us have a voting system. Each of us have websites that we put results on. Each of us have our own registration system. Many of us have poll book systems. Each of us, we've got a similar suite of software that have similar

vulnerabilities that we've got to protect regardless of whether we've got 1.5 million voters or 10,000.

So, because of that, I think we're settling on the idea that the better play is to make sure those resources, those human resources, are getting into each office. The play or the path forward I think is pretty clear. I mean, the Center for Internet Security took a very good look at our ecosystem and laid out some great recommendations for how to secure it. That's not an easy lift, though. That takes a lot of time to digest, even in our offices with our big staffs, we decided we needed to hire somebody who could just own this process for us. We couldn't farm it out to somebody else. So, the human resource is really, really a critical one.

So my suggestion for the local election official, hopefully with a digital defender working in partnership, is to take the CIS or Belfer documents and bring their election security, primarily the digital tools rely upon for like the internet based tools, the public facing websites, results, that's a most likely attack vector, bring it from its current state of security to its future state as quickly as possible.

VICE-CHAIR MCCORMICK:

So, you all run pretty robust election offices, but we have a lot of election offices with one person in them. If you could give them one or two pieces of advice on how to secure their offices. I'll just go down the line. What would that be?

MR. HATCH:

Have a security mindset. You have to, election officials we're already a little bit paranoid. We have back up plans for our back up plans. . .

VICE-CHAIR MCCORMICK:

You're the most OCD people I've ever met, by the way. [laughter]

UNKNOWN:

That's fair.

MR. HATCH:

Amen. We've got to have a secure mindset, and we can't think that it just relates to the voting machines or to the voter registration. It relates to our websites, our Facebook accounts, our personal Facebook accounts. It relates to our email, and the security that we have around that, because that's quite often where the bad guys look first, because that tends to be where we're the most lax.

So, I'd say you start with a security mindset and you distribute that all the way down to the poll workers like you asked about earlier, Chair Hicks, what can they do? My thought is they have a security mindset.

VICE-CHAIR MCCORMICK:

Anybody else?

MR. STAFFORD:

Yeah, I would say the human firewall training. You've heard that term before. The statistics I read or cited are somewhere between 80 and 90% of all attacks initiate through an email. So, if you can address that attack vector, to borrow a Noah term there, then you know you're making some progress there, and particularly if you only have an organization with a couple of email addresses, it's theoretical pretty fairly easy to do.

And then there's a lot of resources out there, even for small jurisdictions. I know, you know, you've got other things that you're tending to, but there are, carve out some time to look at the Belfer documents and the CIS documents and I know it's a lot to -- we're still on very much in the early stages of looking at those and internalizing them and implementing a lot of those recommendations, but there are tools out there. It's just a matter of having of the time and the capacity to go find them.

VICE-CHAIR MCCORMICK:

Lance?

MR. GOUGH:

Yes, and there are a lot of state organizations that are out there that are reaching out to the very local, the smallest local jurisdictions and giving as much help as possible. I know the State Board of Elections has met with their security people trying to get

the word out to everybody. So, it's something that we are actually having meetings constantly where we have state organization, even to meet and discuss this information.

I know Noah spoke at a bunch of them, sent out an email blast to every election jurisdiction in Illinois, explaining what's going on and what we need to look out for. And as long as we keep getting that word out, I think they'll catch on.

VICE-CHAIR MCCORMICK:

Yeah, I mean, when I was at the DOJ we always kind of put on our bad guy hats and thought, you know if I was a bad guy, where would I – you know, how would I pull off what I wanted to pull off, and if we kind of do that ourselves in the local offices, I think Ricky mentioned that, you know figure out where the weak links are in your system and start there. So, thank you all.

CHAIRMAN HICKS:

I'll keep hitting the button until it turns red. So, I want to thank you all for being here today. We're going to take about a three minute break while the staff puts the next panel together, and I can go get an allergy pill. And hopefully stop coughing. So, I again want to thank you all for being here. I look forward to working with all of you.

There was a lot of great things mentioned today. I'm going to check with our General Counsel and see what I can link to on my

personal Commissioner page. So, if there's any information that you want to provide to the EAC or voters in general that we can link to, I think that would be great. One of the great things about the EAC is our clearinghouse function, and so we hope to be able to provide that for voters in 2018 and 2020 moving forward. Thank you.

Again, we're going to take a two-minute break and then start up with the second panel of state election officials.

(Break)

VICE-CHAIR MCCORMICK:

Welcome back and thank you to our state officials who are now joining us. Before we get started, I just want to mention that if you want to provide us a statement, and we have already got one from Doug Kellner from New York, but if you would like to provide a statement, and we urge you to do so, we would love to hear from you, please send it to us at clearinghouse@eac.gov, that's clearinghouse@eac.gov. So, thank you, in advance for those statements. We will read them all very carefully and post them, I believe.

I would like to introduce our state panel. I would like to introduce all of you, and then we can go through the five-minute run through with a few questions afterwards. On my left is Brad King, Brad is the co-Director of the Bipartisan Indiana Election Division.

Brad, the Bipartisan Indiana Election Division provides information regarding the election process, campaign finance, voter registration, absentee voting, and for performing other duties in state election administration.

Brad has served as a senior staff attorney for the Legislative Services Agency, and counsel to the Indiana House and Senate elections committees. He has also served as Assistant Corporation Counsel for the City of Indianapolis. Counsel to the Marion County Board of Voter Registration and State Elections Director for the Secretary of State of Minnesota, so you've got a couple of states there. And I know you went to William and Mary, so I know (inaudible).

MR. KING:

Thank you.

VICE-CHAIR MCCORMICK:

Brad, I look forward to your remarks. Next to Brad is Elaine Manlove, State Election Commissioner for the state of Delaware. Small wonder. The First State. I think you have a number of nicknames for the state of Delaware. Elaine has been an Election Commissioner for the state of Delaware since 2007. Prior to that she spent eight years as the Director of the Department of Elections for New Castle County.

Throughout her vast experience she has seen many changes from both the local and state election process. She has overseen Delaware's electronic signature project to allow voters to have their registration information transmitted in real time from the Division of Motor Vehicles to the Departments of Election in each county. As commissioner she is responsible for the Help America Vote Act funds, the statewide voter registration system, campaign finance and the parent-student mock election. I look forward to hearing Elaine's remarks about Delaware's security efforts. Welcome Elaine.

And finally, we have Peggy Reeves, Assistant to the Secretary of State for elections in my home state of Connecticut. Peggy was appointed Director of Elections for the Connecticut Secretary of the State's office in 2011. Prior to joining the Secretary of State's office, she served in Connecticut's General Assembly as a State Representative, representing the towns of Wilton and Norwalk, where she was a member of the Judiciary, Transportation and Government Administration and Election Committees. Peggy was also a local election administrator for 14 years in the town of Wilton, and with that let's start on the other side. I'll turn it over to Peggy.

MS. REEVES:

Thank you for inviting us to be part of this conversation on election security, and before I begin my remarks, I am going to take a minute of my time to thank you for all that you do, Commissioner Hicks, Commissioner McCormick, former Chair and Commissioner Matt Masterson and Director Newby. You are always there for us to attend our local and state conferences. You have attended and presented at every meeting of the National Association of State Election Directors. We have used your quick start guides, your checklists, your guidelines, your fact sheets. In short, I don't know what we would do without all of you.

So, to whoever is listening, we want you all to stick around and it is our hope that at least one, and possibly two additional EAC Commissioners will be appointed soon. So last fall we were surprised to learn that Connecticut was one of 21 states that was targeted by the Russian government. But fortunately, we have a strong network of protection on the state level as we have been a member of MS-ISAC for many years and we are also protected with an Albert Monitor. Our cyber security defenses held, and the Russians were turned away, but it was a wake up call for us. So, we are now leveraging the services provided to us by DHS, MS-ISAC, EI-ISAC and as well as other agencies to further protect our infrastructure. We are doing real time monitoring of all inbound and outbound traffic to our state network, weekly hygiene scans of

internet facing applications, and a risk and vulnerability assessment from DHS, which is scheduled for next week.

As an additional level of security, our centralized voter registration system is not directly connected to the internet. In order to access this system, the local election official must use a work station that has connectivity to the state network. All 169 towns in Connecticut have a state provided connection to allow for access to the voter registration database.

But Connecticut, like all of New England is highly decentralized. We do not have county government. So, elections are run by 338 registrars of voters, 169 town clerks, for a total of 507 local election officials who oversee our elections and must be trained by our office. And if you add in the deputies and the assistants who work in the local town offices, we are talking about several thousand local officials.

In many respects, this decentralization is a strength because it would be extremely difficult to hack an election. But that decentralization is also a weakness because of possible vulnerabilities in the many access points into the centralized voter registration system. For example, are they using operating systems that are no longer supported like Windows XP? Are we being told if ransomware is being put on their local machines?

Certainly, the state fusion center would be informed of it, but we might not be informed at the state level.

So, over the next two months we have decided to do enhancements to the voter registration database that will be implemented to enhance user authentication, including a stronger password policy and two factor authentication. Also, we will have a new analytics report that will compare voter data over time to look for any anomalies, sort of untoward events that we are not expecting.

In addition, we have seen an increasing need over the last decade for a marriage between IT and elections. Because we have found you have IT personnel who don't understand elections, and you have elections staff who don't understand IT. So, now more than ever we need to merge those two. Therefore, we have asked to create a cyber security election system within our office, consisting of an election officer, with subject matter experience in technology and cyber security, and an IT cybersecurity professional who would have subject matter experience in elections.

We have also recently created a Connecticut cybersecurity taskforce composed of representatives from DHS, the Connecticut National Guard, state government legislative municipal leadership, academics, and local election officials to share best practices for election security and solicit their advice on the expenditure of new

HAVA funds. We are pleased that Congress authorized these additional HAVA funds to enhance technology and make elections security improvements.

We believe that the 2018 election will be one of the most challenging elections we have faced. But we will work with out local election officials to make sure that our systems are secure, and the public has confidence in the outcome. Thank you.

VICE-CHAIR MCCORMICK:

Thank you so much Peggy.

MS. MANLOVE:

Okay, thank you. Thank you for inviting me to speak today, and I want to echo what Peggy said about thank you for just being there for all of us. The EAC has become such a go to place for all of us that it makes a big difference in the way we do our business. It gives us a central place to go to for answers.

So, the first round of HAVA allowed Delaware to introduce electronic signature, the interface that we have made with DMV, the real time interface. It also allowed us to do automatic voter registration, which was kind of a I guess our e-signature was the fore runner to automatic voter registration. Then, on line voter registration. So we used most of the original HAVA funds to use technology to improve the way we do our business every day.

As we move forward with the new funding, as grateful as we are for this funding, our plates are even fuller now than they were then because of security. So, I just want to bring you up to speed with what Delaware is looking at as we move forward. We need new voting machines. When the first round of HAVA funds came out our machines were fairly new, and I got lots of phone calls about what a great job Delaware did because we had electronic voting. We had no paper trail, but we had electronic voting. And people in Delaware were watching TV seeing everybody with the hanging chads, and calling me up saying what a great job Delaware was doing. And now those same people are calling saying where is the paper trail? So, times change.

But as we look at new voting machines, security is a big part of that. As I said, the public is concerned now about the paper trail where they weren't. They also don't understand that it is a process to buy new voting machines. I think the general public sees well you don't have a paper trail so lets just go buy new machines as if I could walk into Staples and load up a cart. So, the public, we used a lot of public input in this. We had a taskforce to review different types of voting systems.

But the big debate again is whether we use - there will be paper, whether we have paper as a - voting on paper, or whether we have the DRE with a Vive pad. That is the challenge at this

moment in time. Thanks to the HAVA funds, I am sure that will be a part of the funds that buy these new voting machines. We are also looking at electronic poll books, something we don't have now, but there is a bill in our legislature now to create early voting and that will necessitate the poll books.

The state, we are on the state's mainframe and they want us to get off the state's mainframe, so we are looking now at election management and voter registration system. And we will look at updating our absentee system, although the one we have is, we bought with HAVA funds and it is fine.

So, we are different than a lot of other states. All of the election officials in Delaware are state employees. Always have been. We used to have four different agencies, but a few years ago they were merged into one State Department of Elections. So, it makes us different. We don't have, while we have county offices, they're not really locals, they are state employees.

So, we work together, we meet once a month and review all of the security protocols. We meet with our Department of Technology. Delaware was one of the 21 states where there was an attempted intrusion. I thank our Department of Technology and Information for providing the security. So, we work with them, and this news time frame has allowed me to find out that we have

always belonged to MS-ISAC as far as department of technology, not necessarily elections.

We do have an Albert Monitor. I went back from the last meeting I was at and said, we need to get this Albert Monitor. Found out we have two. So, I am confident in the security we have, but every day is a new turn in the book here to find a new page of what else is going on that we don't know.

As we move forward, we are looking at the penetration testing through Homeland Security, and I found out, and this is something I have a question for everybody here. Using DHS versus an outside vendor, apparently Homeland Security does not alter their rules of engagement. And Delaware Department of Technology and Information, not me, would want them to specify exactly what areas they are going into and I think in reality, that works, but in the view of Department of Technology and Information they want all of that in addressed in writing, so we're back and forth on that right now, and I'd like to talk to other states during the next couple of days and see what their experience has been.

So again, we are grateful for the additional funding but again, our plates are even more full than they were now because of security, so this is a great help to us. Thank you.

VICE-CHAIR MCCORMICK

Thank you, Elaine. Brad, I am looking forward to what you have to say.

MR. KING:

Thank you, Chairman Hicks, Vice Chair McCormick. It is my pleasure to he here with you. Thank you for the invitation. I'll say it's unanimous. The United States Election Assistance Commission has lived up to its name, particularly with regard to voting systems. I don't know what Indiana counties or Indiana voters would have been able to do or accomplish during the time the EAC has been in operation in improving the quality and confidence in our voting systems without your help. So, thank you for that.

VICE-CHAIR MCCORMICK:

Thank you.

MR. KING:

I was also intrigued during the opening remarks made by commission members, that you both mentioned territories in the Pacific Ocean. The smallest US possession is a beautiful tropical island in the south Pacific noted for its scuba diving named Kingman Reef. Unfortunately, it has no population so therefore it won't qualify for any grants. (Laughter)

But I think that a voter or even an election administrator certainly would have had to have spent the last two years scuba diving off of

Kingman Reef to not have their concern and awareness regarding cybersecurity brought to the fore.

I want to take my remarks to focus on one aspect of security that I think is particularly important for county and local election officials. In Indiana, we have certainly taken the challenges and threats of cyber security to our statewide voter registration system very seriously. Our legislature appropriated funds for modernization of our voter registration system to incorporate new security features as they became available.

But we noted that there were physical security protocols that we could undertake and the counties in our case who maintain voting systems can undertake that will increase public confidence, because it's not a question simply of the statewide VR systems but also of the voting systems that are maintained locally.

And so, as part of the short legislative session this year, Indiana adopted Public Law 100. Public Law 100 focuses on the physical security of voting systems primarily at the county level. It provides for counties to be reimbursed for taking relatively simple and inexpensive steps to develop security protocols ranging from items as relatively inexpensive as alarms systems, video cams, that the state will provide money for as reimbursement.

The legislation also sets forth very detailed protocols regarding chain of custody, ceiling, and other items with regard to

the physical management of voting systems, but recognizes that not all counties are the same. As other speakers have indicated, some have large staffs, they also have large numbers of voting systems or electronic poll books. Other counties have one person, or two persons required for that task. And so Public Law 100 provides for those counties to work with our voting system technical oversight program, based out of Ball State University, and with the election (inaudible) to develop customized, security protocols for that county to implement.

We've also in the legislation provided for various aspects of beefing up the comprehensive inventory we have of individual voting system units and electronic poll books throughout the state. By identifying the specific locations where those are stored and secured, and also requiring that counties certify annually that the information contained in that inventory is up to date.

With that in mind we have addressed the end of life process for voting systems and electronic poll books. When a county disposes of either of those items, it is now required under Public Law 100 to submit a voting system or electronic poll book disposal plan to the state for review and approval. We look forward to making certain that the inventory remains constantly current and further addresed an issue that arose with regard to the distribution of voting systems at the beginning of life. We had an individual

who approached a small voting system vendor in Indianapolis before a highly publicized national convention, requesting to buy a voting system. The individual did not follow through with their purchase, but it prompted the legislature to include a provision in this bill that bans the sale or transfer of Indiana certified voting systems within Indiana, except to the limited case of counties in Indiana who will use them, or other counties or jurisdictions throughout the United States. Thank you for the opportunity to speak.

VICE-CHAIR MCCORMICK:

Thank you Brad. I'll start. Sure, I'll start with questions. And you mentioned just now, vendors. You mentioned experience you have with a vendor. In general, how have the vendors been? They are an important partner in the election community. We don't often hear from them in this kind of a setting. But, what have your experiences been with them? Are they, can they help bridge some of the issues here between states and locals?

MR. KING:

Yes. Commissioner, I think that's true beyond question. The vendors play a key, pivotal role in the security process for the voting systems. I would say our experience has been mixed, particularly with regard to electronic poll book vendors, which is a growing industry. The education process regarding cyber security

threats and physical security threats is not just happening for election officials. It's happening for vendors, and we've noticed a growth curve, and overall a desire to cooperate and help us improve the system.

VICE-CHAIR MCCORMICK:

So, do you think they are taking adequate steps to address the cyber security and the physical security issues?

MR. KING:

I am not confident that all vendors are fully addressing all cyber security concerns. Some of that may be a question of timing and process, and the role of the marketplace.

VICE-CHAIR MCCORMICK:

Thank you. Do either of the others want to weigh in on that vendor issue?

MS. MANLOVE:

I have been dealing with vendors recently and I have been satisfied with their response. Again, when we talk about adequate as far as security, I never know what adequate is. I think we think we are all at some level, but if the bad guys get to another level, I think that's just an ongoing game that we are going to be playing, and I think you know we thought Florida 2000 was a game changer for us, I don't think we've ever seen a game changer like this, and I think it's the new way of life for all of us. So yes, I do think the

vendors are working with us, but I think we are all in the same game.

MS. REEVES:

So, I would just add that I think our vendors in the past have been focused on the physical security of things, so that strict chain of custody of the voting machine and programming the memory cards and everything for our optical scan tabulators, but not so much on cybersecurity, so I think that is something we all need to talk about and perhaps have audits of the vendors themselves. Where they program the cards to be sure that is safe and secure.

VICE-CHAIR MCCORMICK:

Do any of your states do audits? And if you do what do those look like?

MS. MANLOVE:

We do random audits in Delaware. It's not mandated in the code, but I expect it will be going forward.

MS. REEVES:

So, we are mandated to do 5 percent of all the polling places on a random basis after every election and primary.

MR. KING:

We have a provision for audits upon request following an election.

VICE-CHAIR MCCORMICK:

Okay. Peggy, you mentioned the Albert Sensor. This is one of those questions where we know the answers, but not everybody does. Can you tell us what an Albert Sensor is?

MS. REEVES:

I knew you would ask that question. (Laughter) I did write it down a little bit, because I honestly didn't know before now. I think its also called Einstein sometimes, right? But it's a network monitoring system which provides automated alerts of malicious network threats focused on state, local, territorial and tribal, and its sent, so if anything comes up its sent to MS-ISEC for analysis and they let us know. I think basically that is what I have been told it is.

VICE-CHAIR MCCORMICK:

Thank you. What would you consider your biggest one or two challenges or risks in this security environment? Each of you, just one or two things that you are most concerned about.

MS. REEVES:

Well again, I think I have already spoken about our local election officials are terrific, but many of them just work on a part time basis. They may come in once a week. They don't, necessarily, because they are such tiny towns in Connecticut they are not staffed every day. The town clerks are there, but the town clerks are only involved in issuing absentee ballots in terms of elections, so everything else is done by the registrars of voters. So,

my concern is the fact that have very part time people and we have to make sure that they are certainly trained on cyber security going forward.

VICE-CHAIR MCCORMICK:

So, maybe some professionalism issues?

MS. REEVES:

Yes. Yes.

VICE-CHAIR MCCORMICK:

Elaine?

MS. MANLOVE:

I think while we are all state employees, I do think making everyone understand, from no matter what position you have, that cyber security affects all of us, and making everyone aware of the importance of it. And yes, training., training, and training.

MR. KING:

In addition, I would add my concern is with regard to the chain of communication. So often we discover an issue, whether it's one of real concern or simply one of perception, only after it's become a public issue or public question. We encourage, certainly the vendors and our county election officials to inform us immediately of any anomaly so we can promptly investigate it and prevent any concern that's unfounded.

But I think that carries forward with regard to Elaine's point on training. We need to empower the poll workers to ask questions. To say, I am seeing something unusual. It may mean nothing, but I am making you, in this case the county or the state, aware of the problem so that if there is further action needed it can be taken promptly.

VICE-CHAIR MCCORMICK:

So, I will say one more thing, recognizing that incidents can happen and probably will, can our voters have confidence in the security of our elections?

MS. REEVES:

Yes. I would say yes, they should. I mean for example we can state emphatically; no votes were changed in the 2016 election. And I think they should have some faith in the fact that we are moving forward to make sure that we do the best we can to make sure that nothing happens to jeopardize 2018 and 2020.

MS. MANLOVE:

Yeah, I agree with Peggy, and 2016 was a wake-up call for all of us. We didn't know what we didn't know, and now we have kind of marshalled all of the forces available to us to mitigate anything like this. So, I think, yes, I have confidence. I have more knowledge than I had before and yes, more confidence goes with that.

MR. KING:

Yes. I'll join that statement and say that I certainly have full confidence that the elections we conduct throughout the United States are as secure as we can make them at this point. There is always room for improvement. There will always be new technological challenges, but our presence here today is an indication of our dedication to meet them.

VICE-CHAIR MCCORMICK:

Thank you to all of you. That is a question I am asked often when I am out. People ask me, can we really believe in the results of our elections, so I think it's good for us to remind voters that we do and can have confidence in our elections. Chairman Hicks?

CHAIRMAN HICKS:

I want to thank you all for being here today. I have known each of you for a number of years, and I know the voters should have explicit confidence that their elections are being run well by the work that you do in your states. Mr. King, you mentioned audits can be triggered by request. Who makes that request?

MR. KING:

The request under Indiana statutes can be made by political party chairs who might anticipate a re-count being filed.

CHAIRMAN HICKS:

I just want to make sure that it's not individuals just saying, I don't believe this happened, I want you to do an audit sort of thing. So, it has to be one of the political parties?

MR. KING:

That's correct. It's essentially limited to the individuals who would be entitled to petition for a recount or contest.

CHAIRMAN HICKS:

Ms. Manlove, you had mentioned that the state is asking that you leave their mainframe. What sort of, do you have an estimate of timeframe and cost that is going to be associated with that?

MS. MANLOVE:

Not yet. We are working on that right now and I now have an RFP, and we have responses to the RVP, and part of that is the new election management system. In all, when we get down to the dollars and cents of it, we are not there yet. It will happen sooner than later, but that is all going to depend on the cost of the voting machine. Our RFP was four sections, voting machines, election management systems, absentee and poll books. So, depending on the cost is depending on how fast it all happens. My goal is that it all happens at the same time.

CHAIRMAN HICKS:

So, I guess, this is more for all three of you, are you on the mainframe for your particular states, or do you have an individual mainframe for your offices?

MR. KING:

We have a dedicated mainframe.

MS. MANLOVE:

And again, we are on the state's mainframe but working to move off.

MS. REEVES:

And we have a server, but it is all within all of the state's service. In fact, it's in the same area as our state police so we feel that it is pretty well protected.

CHAIRMAN HICKS:

I only have a couple of more questions. I believe there are a couple of more events going on today. We have a third panel going on in a bit.

I want to thank you for the praise that you gave to the EAC, and as chair it is easy to sit here and try to take credit for that, but it's mostly the staff. We have a very dedicated staff and I am very proud of each and every one of the individuals who have come through that door and the work they do for the EAC. So, I think they should be the ones that are bathed in the accolades that you bestowed upon us.

That being said, what more can we do to help you in 2018 and 2020. I believe that with the Congress coming together, which no one saw and anticipated of giving $380 million moving forward. Other than additional resources in terms of funding, what else can the EAC do to help you with your elections?

MS. REEVES:

I would say just keep doing what you are doing. I mean I took a look at your website and there is such a wealth of information there. Almost too much. I mean you could spend days looking at everything you have, and I think the more that we can get the word out to local officials to use your website, because it's terrific, so I would say just keep doing what you are doing.

MS. MANLOVE:

I will echo that. It is a great place, we have a place now to go when we need information, or we have somebody to pick up a phone and call and say I need help with something. That's a great asset for all of us.

MR. KING:

In addition to those, I would add continue the efficient manner in which you have begun the process of educating us about the new funding. Work with us as we have questions, and I anticipate that we will be able to use that money in the best interests of the voter. Thank you.

CHAIRMAN HICKS:

Do you have any additional questions? I want to thank you all for being a part of this. I have been invited to two of your states, and I hope to come. I guess it's going to be the first Monday of each month and then it's going to be in September, hopefully, that the clerk's association is going to have me in Connecticut. I want to thank you all for being here and thank you for what you do, and I look forward to seeing you tomorrow with the Standards Board.

With that, I wanted to open it up for the audience. If you are an election administrator or an election person. Natalie from our staff is there and you can line up behind her. We are going to set the timer for five minutes each. So, if you want to step to the podium, I ask that you give your name, your affiliation with the state that you are with, and limit your comments to five minutes.

We will try to get as many, if you want to use the podium, or you can sit at a seat. We want to limit as much as possible. So, they want you to use the podium. So, if you can turn the other two mics off, if you turn the other two off, that one should come on. There you go. When it turns red.

MR. SHELLMAN:

I can program a voting system. I can not operate a microphone. Thank you. My name is Dwight Shellman and I am

the County Regulation and Support Manager for the Elections Division of the Colorado Secretary of State's office.

Thank you very much commissioners and chairman for hosting this forum. It is an important dialogue to have. I did want to just make kind of a couple of pleas to various constituencies that I think are important in the process. Commissioner Hicks asked at the conclusion what more can the EAC do? And I think there is an important area of substantive leadership here for the EAC. Every state and local election official in the country is confronting similar threats in different models in different circumstances in their own individual jurisdictions. But the threats are common, and rather than having 50 states and territories and 6,000 local election jurisdictions recreate the wheel on all of these elements, I think there is some commonality that the EAC can provide some resources for.

For example, an on-line cyber security training for state and local election officials and poll workers. And I think as Noah pointed out this is, we are all as strong as our weakest links. And because of that such an online course, if it could be tested, and a certificate issued, that might help us all. We could send our locals to that resource to accomplish that particular objective. And I am sure there are many other ideas out there.

My next plea is to the election integrity advocates. I think it is very important here to remember that technology enables state and local election officials to make voting as easy as possible for voters. And that is a very important value to election officials. And technology however, always introduces additional vulnerabilities. So, I would just encourage the advocates to understand that we really need to do this with a trust but verify approach. It's okay to use technology, but the technology must be used wisely and knowing its vulnerabilities and making sure we mitigate those vulnerabilities.

And I raise that because so much of that dialogue here I think is counterproductive. Messaging matters. And the Russians aren't going to have to hack a single thing if the messaging results in our citizenry just concluding that it's hopeless and we are all vulnerable. That is absolutely not the case.

And then my final plea is a plea to the systems providers, both voting systems and the dependent election systems. Hopefully they understand, and I think most of them do, that they are now providers of critical infrastructure and trust but verify applies to them as well. They are very important partners in delivering election services, and I know many of us really hope that they will collaborate with us on those efforts, and we really need that from them.

Finally, I just wanted to mention that immediately after this forum the Brennan Center for Justice is hosting a panel in the Cadiz Room on the mezzanine level, which will just be a panel discussion where we can get in the room and maybe talk through some of these issues. Trey Grayson, the former secretary of State for Kentucky will be moderating that. Doug Kellner of New York and Liz Howard, formerly of Virginia, will be on the panel as I will be as well, and its just an opportunity for us to get in a room together and start brainstorming about maybe the best way to approach this issue and strategies to prioritize our various needs.

CHAIRMAN HICKS:

That is going to be here in the hotel?

MR. SHELLMAN:

Yes, it will be starting at 4:15 and it is just up on the next level in the Cadiz Room. And refreshments will be served. Thank you.

MR. KELLNER:

Good afternoon. My name is Doug Kellner. I am co-Chair of the New York State Board of Elections. And I will join Dwight's invitation for those of you who would like to join us in the Cadiz Room, one flight up to continue these discussions.

I have submitted a lengthy statement which I hope will get published eventually, and so I will just focus on two or three small

points that I think have not been discussed so far. Governor Cuomo in New York has been very proactive in recognizing the security threats. He made this a priority in his state of the state address, and also in the most recently enacted budget.

One of the innovative things that was added to New York law was to require disclosure of independent expenditures for internet ads. I understand that Seattle, Washington has had that requirement for many years, but I think New York is the first state to actually implement it. It will be very interesting to see how those disclosure requirements actually affect spending and the fact that we're required to put up all of these things on our own website leads me to wonder what will happen. Will the state board of elections in effect become a clearinghouse for political advertising in New York as a consequence of that requirement that we actually post all of the ads?

A second thing that I wanted to talk about is that many of us have been advocating on the need for voter verifiable paper audit trail for many years, and many states have that voter verifiable paper audit trail. The audit trail is only useful if in fact there are audits, so audits are a very important aspect. There are many different ways to conduct audits, and one of the interesting issues that has been arising recently is that there are about half a dozen states that have scanning systems that record ballot images and

where those states allow those ballot images to be accessed by the public. I think that's a very important area. We just had a court decision in New York which will allow New Yorkers to obtain copies of ballot images by the Freedom of Information Law, and what that does is it gives the voters the right, in effect, to do their own audit, because they can go and take those images and do their audits, and in the long run that increases the confidence in the system. Many citizens have accessed ballot images in the various states where it's been allowed, and have done those audits, and those audits confirmed the outcomes of the elections. And having that kind of transparency and verifiability is one important way to increase confidence in the elections, and by having that audit capability that of course makes it that much more difficult to hack and challenge the outcome of an election. So, thank you.

MR. ROCK:

Good afternoon. Chairman Hicks, Vice-chairman McCormick. My name is Rob Rock, Director of Elections for Secretary of State Nelly Gorbea, in the state of Rhode Island. I first want to thank you for hosting this meeting.

Much of what I'm going to talk about quickly I think I'm last, so I'll be brief. But much of what I'm going to talk about is what Rhode Island is doing to secure elections in the state, and much of it we've learned at these type of meetings from other states. So, it's

been very helpful for us and hopefully we can be helpful for others. When Secretary Gorbea got elected in 2014 and started in 2015, one of her top goals was to modernize elections in Rhode Island, and one way that we are doing that is on the cyber security front. Just last Wednesday we held a briefing for members of the public and for the media regarding what Rhode Island is doing to ensure our elections are as secure as possible, and came out with a report which I'll reference briefly and also send to the EAC for reference.

But essentially the report outlines the work Rhode Island has done over the last three years in three specific categories. One is online systems, the other election day operations, and the other is human resources. And I want to make it clear it's been a collaborative effort in Rhode Island. Secretary Gorbea feels it's very important we have as many people at the table as possible. So, a lot of the stuff we've done have come with the help of the General Assembly, the Governor's office, the Board of Elections, our local election officials which I'd like to take a moment to recognize Louise Fanoff who is our local election official here today at the Standards Board. It's her first meeting, so welcome Louise.

Quickly I want to talk about how we're securing our online systems. The Secretary of State has taken a variety of measures to greatly reduce and mitigate the threat of cyber-attacks, and one of the ways we are doing that is like many states, partnering with the

Department of Homeland Security under the critical infrastructure designation to further protect our central voter registration system by testing for vulnerability, sharing cyber security information, threat incident reporting and receiving ongoing risk and vulnerability assessments, that include penetration testing, web application testing and social engineering.

We're also working with our state's higher education institutions. We are very fortunate in Rhode Island to have quite a few nationally recognized institutions of higher learning, for example, Brown University, and Salve Regina University we worked with closely on cyber security and computer science matters, and they've been great. Having academics at the table has been really helpful for us. We're also working with other state partners, such as the National Guard and the state police's fusion center, who have both done assessments on our voting systems and offered recommendations for ways that we can protect ourselves even more. So, it's been great to partner with other state entities because, again having as many people at the table as possible we feel is very important.

Election day obviously is very important. And in 2016 we procured new voting equipment with the ultimate security measure and that we have paper ballots. We've had paper ballots since 1998 and we'll continue to have paper ballots, so we're fortunate there.

We're also, in 2016, we rolled out a pilot program for e-poll books and in 2018 we're going to roll it out for the entire state, and our electronic poll books utilize a proprietary encrypted application running on Apple's ISO software which meets the security requirements for the federal government secure network such as the Department of Defense and Department of Justice's data applications.

We also passed in 2017 an audit law which is very similar to what Dwight Shellman and his team in Colorado successfully launched last year. We have a risk limiting audit law that we are going to be rolling out over the next few election cycles which we feel is very important.

And then finally, securing our human resources, we've worked quite intently to make sure all election officials at the state and local level have the knowledge to prevent threats and assess problems. Local municipalities have a variety of technological expertise, and it's imperative local election officials can speak articulately about elections security and help prevent attacks on our systems.

So, in 2017 in October, we convened all the cities and towns for a cyber security summit, and went over cyber security protections and making sure passwords are safe and make you don't click on emails and attachments from people you don't know

and things of that sort. It's very important that we train our state and local election officials on that, state included as well. We're going to continue to do those cyber security summits.

We also, within the Department of State, began a phishing campaign to test and educate all of our staff, not just elections, but the entire Department of State staff to be sure that we know how to handle emails and passwords and things of that sort. It's very important. And we're also going to be involved in the secure the human program, where all of our employees are going to be trained on the best practices for cyber security.

So, I'll end with federal, state, and local government cannot allow cyber threats to election systems, whether real or perceived to undermine the role voting plays in our society. Despite the progress made over the last three years, it is important to remember that cyber security is not a destination but a continually evolving road that requires constant attention to mitigate risk. We must always strive to do better for voters because a single act of casting a ballot is fundamental to our democracy and fundamental to making government accountable to the people it serves. This will require a continued commitment and a corresponding dedication of resources to ensure the integrity of our voting systems.

And I apologize for going over my allotted time, being last. Sorry. Thank you.

VICE-CHAIR MCCORMICK:

Sure. Thank you so much. While I was sitting here, just an observation, you know, 18 years ago this was ground zero. South Florida. In the Bush v Gore race. How far this community, this election field has come since then. It is remarkable, and I appreciate all the professionalism in this room, the excellent comments and questions that we've received today, and just want to thank you all who are in the election field for your hard work and your continued dedication as public servants to our representative democracy. Thank you.

CHAIRMAN HICKS:

Thank you, Commissioner McCormick. I want to echo that, but also add that those folks born during that 2000 election are now going to be eligible to vote. So, keep that in mind as we move forward with 2018. (Laughter) I want to thank you all for joining us here today in Miami and online. All the statements delivered today will become part of the EAC's official record and available on our website. For those watching, statements can be emailed to listen at EAC.gov. And for -- or -- oh, yeah. Or clearinghouse –

VICE-CHAIR MCCORMICK:

Clearinghouse@EAC.gov

CHAIRMAN HICKS:

For more information about the EAC and our work on this and other topics please visit EAC.gov. With that, we will close this forum and move forward with the rest of the Standards Board and Board of Advisors.

(Applause)

(4:13 p.m. – RECESS)