>> Chairman Hicks: Let's start again. [Laughter] I'm so used to hearing my own self speak that I forget no one else can hear. Welcome to Miami. To all here in the studio audience and online, welcome to the forum we're having today on U.S. 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 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's 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?

>> Commissioner McCormick: Thank you, Commissioner Hicks. I am Christy McCormick, vice chair of the EAC. I'd like to ditto Chairman Hicks and welcome you all to our EAC forum on election security and to those online, 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 gives us information and perspectives on how we can serve state and local election officials as they run our country's elections.

I would be remiss if at this also did not acknowledge the Trump Administration and those in Congress, especially those whose leadership helped secure the $380 million in HAVA funds prior to the 2018 election this year.

We are very thankful for Brian Newby our executive director and Dr. Mark Abbott EAC grants director and our other staff members who have surpassed any other effort that I know 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 state officials to inform them of the amount of the appropriation that their states would be receiving, and received the whole gamut of reactions to that news. But I want to report we're 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 18 years and are continuing to change and we're in a completely different environment even in this past two years. Election and security is now at the forefront of the minds of all election officials across the country and I'm 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 they will give us today help us serve the election officials even better.

I'm going to turn this over to our executive director Brian Newby but also want to urge election officials 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 or our staff online or on the phone and we'll do whatever we can do assist you in this important effort. So thank you again for being here. And I'll introduce Brian Newby, Executive Director of the Election Assistance Commission.

>> Brian Newby: Thank you, Commissioners. When we first came up with the idea of this forum, the thought process was that there are 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 election 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 will conduct IT training for election administrators and created a video that election administrators can show to explain how election security works before they get into the specifics of their jurisdiction. I think we were all disappointed when we had the government shutdown leading to our cancellation of the earlier meetings in January. But that process actually manifested itself into the omnibus appropriations act in March which then included the three hundred 80 million dollars in grants or HAVA funds for many things including election security.

And gave us the opportunity now to be able to speak to that as part of this forum.

So that's what we're going to do now in a moment. I'm hand it over to Mark Abbott who has done a terrific job getting the money prepared to be distributed to the states. I want to show you one quick map. Gives you an idea how the funds are spread out. The more green you see, the more green the states get basically. And that's about the level of detail I'm prepared to explain here right now. So I'm going to now hand it over to Mark who will get into all the details of the process.

>> Mark Abbott: Thank you, Brian. Thank you, Chairman Hicks, Vice-chairman McCormick. Pretty much the opportunity to speak with you and our election officials across the country today about these grants. The EAC team has done just a ton of

work in the last three weeks to get where we are today and I'm happy to give a brief overview of the process for getting the money, for putting together some plans on how you're 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've had money appropriated by Congress and the last money we received was section 251 requirements payments to meet the actual requirements of title three. So very specific purpose on those grants.

Section 102 was replace 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 administration of elections and things you could do with money but it was the most flexible type of money available to the states at the time. And really put the onus on them and because they knew best what they needed in their state and allowed them to administer these funds to improve their federal election processes.

So it became apparent we were going to get additional money for improvements to elections we thought 101 was the place money might go. Congress agreed with the staff and were able to make the appropriation of $380 million signed on March 22nd under section 101 of HAVA. This money needs to be expended by 2023 so it's not here forever. We have five years to draw down and use the money.

The issued April 17th, which I thought was a good day since mostly uncle many Sam as it weighing money but we were able to give a fair amount back. The award pacts has the notice of granted he award a legal document that allows states to access money and gives them the requirements they have to follow to if they're going to take the money and then some instructions on how to draw the money down from their accounts at the treasury and then somewhat uniquely we have this 90-day deadline in

there. 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're 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 funds and have the money in three to five days in your account at your state to spend on immediate needs that you know that you may have in the run up to the 2018 election. So even as you're 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 administration of your federal elections including enhance technology and make elections security improvements. So election security is on everyone answer mind. It's been tremendous amount of press on this topic. And I'm happy to say that the 101 funds are probably the best vehicle we have at the Election Assistance Commission to allow states the flexibility and speed to put in place what they need. So you can improve administration generally it's a very broad category and on the website you'll find all kinds of examples of how states have done that in the past and what the EAC has said is 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 -- that's for language accessibility as well as handicap accessibility -- the quality and quantity of your polling places. There's a broad gamut 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 in positioning for a more secure vote is around communication and training and 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're getting lots of good ideas from states now on how they plan to use those funds. We will post those ideas on website and share as broadly as we can as innovative ideas roll in from partners and states.

So that's a brief overview of the funds. I think the highlights are as 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 monies available now because we know the issues are now.

So that's it, my part. I can answer questions and I'll be available afterward. One other thing. I also have with me Mike Kanifec [phonetic] for the Election Assistance Commission. He's been contracting with us for -- since 2010, he knows HAVA very well and funds well. He helps with their audit resolutions he's available today and through Friday to answer questions and help states get ready to put their requests the funds and begin spending them. Thank you.

>> Thank you, Dr. Abbott and executive director Newby. I have a few questions, more of making sure that those folks out there in the audience and online who have these same questions get those answers. These are some of the things I've been hearing for the last 40 days or so since the President signed this March 23rdrd.

When is the money available?

>> 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 election 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 form the U.S. treasury as long as they do it within five years

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

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

>> 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 it has 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?

>> That's correct. So 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. Didn't do that in this case. They said we want you to work on security, we want to you 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 as the state level.

So that's how it was decided.

>> Well, if I could just add, I think -- our view is for two aspects. I think for one, we were going to judge our success in this in terms of EAC and how fast we get the funds out and then how efficiently we could 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, this can -- there are very few restrictions on the way these funds can be used and Mark it an expert in knowing what those restrictions are.

>> And so I've 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 basically was the same as the color of the at Atlantic and Pacific oceans meaning the at Atlantic and Pacific are going to be get zero but each state will receive at least how much?

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

>> Thank you. Commissioner McCormick?

>> Just want to clarify the territories are not getting 3 million, right, just getting $600,000?

>> So the 50 states which -- the 3 million is the minimum for small state minimum and then if you're a U.S. territory, not Puerto Rico, the other territories, you get $600,000 in federal funds.

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

>> That is correct.

>> So there's a five percent match, could you give us the sort of outline of that 5% match?

>> 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 and there's a match. Five percent of the federal share. So on the chart we posted on website you can see what your match obligation is but you don't need that match obligation up front. You need to produce that match over a period of two years.

So we'll look for that documentation on your federal financial report the states submit to us annually, the match can be cash or on in kind. In this case an in kind contribution would be something else that you're approving or doing with non-federal money that's aligned with what you're doing in your grant that can county as your match so the match can cascade down to the local level.

So we know we have every locality is working on security as well. They may well easily have the 5% they would need if the state chooses to put some of the money they've received down for the local level to be spent there

>> If they've already spent the money in this fiscal year can they use that as a match prior to had this bill being signed?

>> There is a question of when the grant actually starts on -- when the President signed the bill. The omnibus appropriation goes back to the beginning of the fiscal year so states should contact my office if they want to have costs that were incurred

after October 1st, 2017, included as match or part of a federal share. We'll work through those and adjust their awards as needed.

>> Make sure they will pass audits, right?

>> That's correct. I didn't mention the audit. You know, obligations here. It's been a long time since we've had new money but there are a series of audit obligations states face in accepting these funds. Our office the grants office is 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 the using the money for the things they need to get done, not worrying necessarily about the audit situation for them. We'll make sure they're well educated and have the material they need to be successful

>> The narrative goes to that audit situation right? That's documentation so that they have some sort of documentation to show when they get audited they're appropriately using the money.

>> That's right we need an audit standard. So the standard is found in OMB circulars, tells you have the kinds of things you can do and not do with federal money. What kind of recordkeeping you need to keep, for example, the three-page narrative and the corresponding budget is allows us a guide for -- to audit against. So if you do these activities and if you say you're 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 -- is not reflected in the activities that will be questioned in an audit so those standards are -- you're setting your standards for how you want to spend the money and the auditors will audit against what you said

>> Can they update or amend --

>> As needed. And I fully anticipate doing rounds ever revisions, I think after you hold an election, you see things you didn't see before and you may want to deploy these federal resources against those needs. That is absolutely allowable and encouraged.

>> I know Congress wanted this money specifically to be used as soon as possible and that's 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, hopefully spend it, but if they don't spend it can they hold onto that money or do they actually have to spend it --

>> We have set a five-year period for these funds. The EAC's grants office expectation that you're 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 they weren't aware of yet allowable under the law we don't have that same reflect this year. If Congress wanted to give us that flexibility they could in the appropriation. They did not. So we're putting everything on this five-year clock and we want to help them get through this money in five years

>> 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 for a rainy day fund, so I appreciate that clarity and would urge the states to work with Mark and our staff to make sure that the way the monies going to spent will be appropriate and the that they will be able to pass the audits that the federal government requires. Thank you for that.

>> Thank you.

>> I want to thank you both. 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

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

>> And if I could one thing we had like on 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 serious for clear house that explains and promotes uses some have for this money.

>> Okay. Thank you.

>> Thank you.

>> Thanks very much.

>> So now we're going to have the local election officials come up to the table and after that we're 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're doing in terms of security.

And as these folks get situated, 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 and on, but we don't want to go all night so the clock is going to be set for each of you for five minutes.

The green light is your -- David, I'm look 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 actually will make a noise.

So -- so that being said, I want to introduce our panel here today. Starting on my left, Lance Goth executive director board of elections Commissioner for Chicago. He's been the executive director managing voter registration, election administration for 1.5 million voters for three decades. Including the recruitment and training of 2,000 high school poll workers in every citywide election. Being the first major jurisdiction to utilize electronic poll books in every precinct and lobbying successfully for online voter registration. Election day registration and online 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 Weaver County, Utah. Ricky was elected auditor for Weaver County in 2010, honored by fellow county auditors as Utah's 2013 auditor of the year. In 2015, clerk of the year. Ricky previously served as information system auditor and consultant for price water house for parametric technology corporation and financial analyst for jet way. Thank you Ricky for being here. Noah Praetz [phonetic]. Serves as director of elections in Clark County one of the largest jurisdiction in the country each year team services 1.5 million voter 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 works his way through the ranks during nearly every election job in the department, learning the pain points and opportunities while going to law school at night.

He became deputy director of elections in 2,007 and appointed director in 2013. A board member of the international association of government officials along with Ricky. He also serves as the election center and Illinois association of county clerks and recorders. He has presented on stability, Election Day management online registration, voter registration modernization and other election-related issues. Today he will deliver his marks on election security. Last but not least, David Stafford is the supervisor of elections 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 policy working group and board member of the national advisory board elections systems and software and as a member of the technological and elections working group for the U.S. Election Assistance Commission. He previously served in the northwest Florida director of U.S. senator Connie Mack chief of staff for Joe Scarborough, and director for federal affairs grocery manufacturers of America. Thank you for being here today. And Lance, we can start with you.

>> Yes. Thank you, chairman -- thank you. Thank you for the opportunity to testify in front of the Election Assistance Commission.

To both Commissioners, it's a pleasure to see you again.

Those of us with decades of experience in the election administration have weathered many changes. Introducing of new voting equipment under HAVA, introducing of election early voting, expanding use of vote by mail, and some jurisdictions electronic poll books and online -- election day registration and soon automatic registration. Clear the newest challenges needs 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 into my home state, the state of Illinois, state board of elections voter registration database.

To me, this was just as significant as the problems we experienced with punch card voting.

After hacking in the summer of 26 affected no individual's voter registration records. Hacking had no effect on no individual's voting records. It was -- it had no effect on balloting systems. The Illinois registration system is merely a gathering reflection of 109 counties that feed their data into it. So none of those were hacked at the time.

Which brought a problem that we had. The Russians with the Russians managed to do something that really caused a major problem. They undermined the faith in our franchise. Similarly, in Chicago, we had an exposed in the summer of 2017. I received a call on Saturday in fact the person 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 none of this data got out. In fact the only person that saw this data was the 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 that same -- next day, spoke to the media, explained what happened, that no data got out. But because of that it's left us wide open. What we need to do is concentrate more on who has our data.

This was a vendor that's been an election field for many years. And after that happened we had a 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's out there on the web. I know we have to have person's name and address, but we don't have to have their birth of date, we don't have to have their last four digits of social security. So what we're doing is we're going to scale back on any data that's going out. So in case if somebody ever did get into the system which I'm hoping it will never happen again but who knows, with what's going on right now, we had word that we see that people are hacking into people's home computers now.

The routers are being hacked into. This is something that we need to really take a look at.

So I just want to say that we're going to reduce the number of stuff that's out there, we're going to 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 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'll happen, that we'll be prepared and that nothing will get out. So thank you for letting me speak. We're looking at least risk management. We're looking at the least problems with getting that information out there.

I tell ya --

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

>> Very good.

>> The timer itself is going to be -- it blinks at two minutes, and then one minute it starts doing the yellow beep. Ricky, whenever you're ready.

>> Thanks for having us here and having this event. The biggest cybersecurity security we face as election officials isn't a piece of technology. It isn't even a thing we can purchase and install. It's 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 further down. We've all seen it. But when it comes to trust in government, gravity changes course, trust flows uphill.

Let me explain. There are a couple polls one from Gallup that shows that 71% of Americans trust their local government to handle problems while own 62% of them trust their state government. And the number drops to a dismal 31% for the federal government.

Trust starts locally and flows up the mountain.

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's 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 mountain at the state capital or back in Washington, D.C.

Voters trust in the nation's elections process is driven by the voter's experience with their local election office. Whether it's registering to vote or 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 official. Local election officials are the face and voice of our nation's elections infrastructure and they're what drive the fundamental level of trust in every single election.

This is how it should be. But it does present a chapel. The very level of government that the voters trust 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 studied federal legislation and participated in cyber securities over the past couple 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's just a mindset that needs to be examined.

I realize I sound like I'm griping, like I'm saying 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're 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 cybersecurity experts. Over two-thirds of them have fewer than 20,000 voters. Only 300 of them, about 3 percent, have joined the election infrastructure information sharing and analysis center.

I'll bet about three fourths of them haven't heard about that yet. Our challenge is to figure out how to support the local officials where the training, technology, and funding so they can ensure 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 they don't all stop at the state level. Of course, most states are the keepers of the voter registration databases, which are critical to the integrity of the election. They absolutely need funding to ensure these voter rolls are secure but 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 will help local election officials properly implement cybersecurity tools and educate the public to ensure that public trust in the elections process stays strong. Fortunately the EAC and DHS are been working with state and local election officials and organizations pitching in. IGO has a webinar tomorrow to show officials how to use specific free private sector resources to help stop DDOS attacks. We appreciate being involved from beginning and we commit to bringing our A game with us as we work together federal, state, and local election officials to strengthen public's trust in our nation's election infrastructure. Thank you.

>> Thank you, Ricky. Noah?

>> Okay. 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 adversaries like county sheriffs sent to repel an invading army. Many locals in the election community are pressing for resources first for better technology and routine hand counted audits to give confidence that digital results are accurate. And second, and more critically today, we're pressing for topnotch personnel with skills to navigate the cyber minefield. Our country's local election officials need direct, human support as we work to defend ourselves against the onslaught of digital threats we've been warned about. Over the past 15 years, our office has tried to lead on technology and security. Using applied forensics, creating widely circulated cybersecurity 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 in the Defending Digital Democracy program at Harvard's center to help adapt their digital security expertise to the unique context of elections.

As co-chair of the counsel that homeland security created to help address this election security effort, I've worked with federal, state, and local leaders in elections, technology, intelligence, and law enforcement. In all 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 worked with our colleagues and my friend Lance at the Chicago board of elections to share the cost of hiring a digital security expert. I simply can't fathom how our election officials can meet a foreign threat without a similar support or a similar investment. It's a hefty investment. But defense of digital systems is very difficult. Just ask Uber or Equifax, Boston or Baltimore, the EAC or OPM. Congress just released $380 million to combat election cybersecurity threat and that's 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. 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 bay handful of incredibly dedicated, hard-working heroes, but just a handful of heroes making critical security decisions are Outmatched Against the threats we've 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's lots of low hanging fruit. Second, the digital defenders will work with outside vendors who

provide much of the election's infrastructure to eliminate or defend specific vulnerabilities. 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 analysis center. Third, build a culture of security that adapts to the evolving threats we face. This massive reinforcement effort can be accomplished and 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're bracing against the renewed attacks we've been told to expect. If we fail to get experts into local offices who will help the locals shore up our defenses we'll 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 those are ripe targets for adversaries. A successful attack against those services play not change a single vote but could still damage public confidence. This is particularly true at a time of great suspicion disappointing gracelessness and highly partisan grand standing. Losing candidates are already apartment apt to call their defeats into doubt. A new digital breach no matter how far removed from the vote counting system could turn sore losers to cynicism, disbelief, even revolt. That's the reaction 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.

>> Last but not least, David.

>> Well, I feel like I should welcome you all to Florida, although I'm closer to Dallas, Nashville, and Charlotte North Carolina than I am to Miami. You're no strangers to the state. I support your efforts over the years. I want to talk about what's going on with government coordinating council and work with Department of Homeland Security with our state and local partners and then talk about what we're doing here in Florida. The GCC is making what I believe is great progress although 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 lightning speed in my humble opinion. The sector coordinating council was formed shortly thereafter and then we immediately got to work. I happened to serve along with my two colleagues theory to my right Noah and Ricky on the government coordinating council and we began to get to work very quickly. There's a working group established oncoming one the 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 a decision made that that pilot was successful so now we have established the EI ISAC. And I don't want to steal Amy's thunder from NASED, but as of information I received today, 47 states, 2 territories, 376 local election offices and three associations are now members of the EI ISAC, and I'm proud to say that Florida, 55 out of 67 counties are members.

So lots of great work going on there. Generally I think that the relationship between 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 time has gone on and officials began to work together with each other, I think there was a level of trust that's building and continues to build. We're not fully there yet, but I think that the partnership is working well. The GCC also I think importantly represented -- ample representation 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's a significant presence of local election officials who are on the front lines, which I believe is very important.

Again, in that communications piece something that sounds really easy, yeah, of course we should be sharing this information but once you start scratching be neat the surface how does that framework actually, what's it look like, what does an incident that meets

the threshold of -- require on to be shared and how does that mechanism work is more complicated than that. Great progress is being made led by Ricky, restrictions 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's wonderful that Congress appropriated that money and it's even better that money is going to be getting out quickly. Congress has also been involved in proposing legislation. One word of caution there. In my opinion, when you start getting too specific and statutory language for instance the audit provision that was in one of the main -- the one main pieces of legislation that's being proposed, would require I did a little analysis, 22% 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 to be enshrined in statutory language. Let me talk a little bit now about what we're doing here in the state of Florida. We understand the role 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, 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, National Guard and others there present. So we also are taking advantage of a lot of the resources out there from the aforementioned CIS playbook, defending digital democracy play book, as well as other efforts like cloud flare's project and Google's project Shield. So we understand that we're on the front lines, we're working very extremely hard at shoring ourselves up and look forward to continuing the work with our state and federal partners to ensure we're in the best position we can be for the 2018 elections and beyond. Thank you.

>> Thank you, David. I have a few questions, but before I get into the questions, I want to say thing all for serving as local election officials. A couple weeks ago I had an honor to go to dear friend of mine's memorial, Wendy Noran 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 want to thank you all for being part of that because I know that it's 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 the work that you do.

So with that, I have just a few questions.

And starting with Ricky, David mentioned what's the gold standard in terms of audit numbers and he mentioned 22%. What's a typical number that's used for audits overall?

>> Well, before I became an election official I was a financial auditor actually in 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, 60 items to select, that provides sufficient coverage assuming it's a statistical sample. I don't pretend to say 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 5% as the threshold we look at. And conduct audits on. And those are statistically selected at the state level and then communicated down to the counties.

>> A couple of you mentioned Belford Center and Google and cloud flare and a couple other things. I know that Microsoft is now doing something in terms of defending digital -- defending digital something or other but 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?

I say that because I know that it's not you, Lance and Noah, you come from a large jurisdiction, you know, 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 IT -- for election officials, giving them a basis of what they need to look out for, moving forward with this, and some of this can be found on our website at EAC.gov. But I'm 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?

>> Generally, what I've found is that I've yet to find somebody that tells me no when I picked up phone and asked them to help. I'll give you a for instance. We happen to have University of west Florida in my county and they've got a center for cybersecurity there that's recognized regional center. And it was just one of those things, hey, this is now becoming a really important issue so I just picked up the phone and 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 went through a training. So really in depth training session there to see if this is something that could be modeled or modified to work with state officials. Local officials around the state. So there's a lot of resources out there just going out and asking people. Because one of the things that everybody is I think has pride and understands the importance of elections in the United States. So when you call and ask them, hey, I'd like your help, I'd 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's been a willingness out there be everybody to pitch in and say yes, it's important we secure our elections and let us help you.

>> 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 waiting services that are more robust but they've given every indication those services are available to election jurisdictions large and small which is great.

>> One of the problems is, let's take Illinois, for example, we have a hundred nine different election official that is 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. We need to 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 we need to get down to the smallest jurisdictions because those are the ones that are going to be attacked.

>> 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 GCC 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 how much knowledge -- in a big office we're able to 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 the local election official's office, people who have the capacity to accept a threat and then to work through all the free resources that are already there.

>> Commissioner 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 jurisdiction and 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 laser-ly 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?

>> Depends on what kind of system you're talking about. Like voter registration system is -- let's same 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 system 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.

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

>> They are not.

>> And so we've got voting registration systems and then we've got actual voting systems then we have tabulation systems, election night reporting systems,

>> Uh-huh.

>> Do we look at all separately or as a whole? David? What's your thought? Do we look at it as one single system?

>> I don't think we look at it -- I think we talk about election systems and I think it's important verbiage. Voting systems and election systems respect not the same thing. And I think two 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 focused 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 will -- as you would in a private sector. The other, I think, thing that -- integrator realization -- I think Lance touched on this earlier is we've always been focused on security. And the main

focus has been on what I will call traditional election security owe polling place and ballot security, security of your voting equipment --

>> Physical security

>> Physical security, correct. Now I think there was a -- 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 -- 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 I will annoying 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 what they think it is or should be. How do I know that's gonna happen? Because it happens in every election. And that in and of itself doesn't mean that election has been hacked. I think we all have a level of responsibility to be very careful in the words 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 anticipated --

>> 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

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

>> 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?

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

>> I understand.

>> 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's line and with whom do you share it? If my county comes under attack, should Noah know that? Well, it 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. DHS has looked at it. And I think the document will be very -- it has to be somewhat general but it has a sufficient says physical at this 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

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

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

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

>> 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, but what the ecosystem right now needs is a more equalized or distributed model. In Illinois each of us have a voting system, each of us have websites that we put results on, each of us have you are on 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 Belford 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 from its current state of security to its future state as quickly as possible.

>> 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 advise on how to secure their offices, I'll just go down the line, what would that be?

>> 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 --

>> Most OCD people I've ever met, by the way, [laughter]

>> That's fair.

>> Amen. We've got to have a secure mine set and we can't think that this 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. I say start with a security mindset and distribute that all the way down to the poll workers like I asked about earlier, chair Hicks, what can they do, my thought is they have a security mindset.

>> Anybody else?

>> Yeah. I would say the human firewall training, you've heard that term before. The statistics I read or cited 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'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. You've got other things that you're tending to but there are carve out some time to look at the Belford 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. Just a matter of having of the time and the capacity to go find them.

>>

>> Lance?

>> There are a lot of state organizations that are out there that are reaching out to the very local, 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. As long as we keep getting that word out I think they will catch on.

>> Yeah, I mean, when I was at the DOJ we always put up on or bad guy hats and thought if I was a bad guy, where would I -- how would I pull off what I wanted to pull off. If we do that ourselves in local offices -- Rick you mentioned that figure out where the weak links are in your system and start there. Thank you all.

>> I'll keep it -- so 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. 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 our 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.

>> Thank you.

(Break)

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

(Break)

>> 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, we've already got one from Doug Kellner [phonetic] from New York. Please send it to us at clearinghouse at EAC.gov.

So thank you in advance for those statements.

We'll read them all very carefully and post them, I believe.

I'd like to introduce our state panel. I'll just 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 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's also served as assistant corporation counsel for city of Indianapolis, counsel to the mayor I don't know county and state elections director for Secretary of State of Minnesota. So you've got a couple states there. I know you went to William and Mary so I know --

>> Thank you.

>> Brad, I look forward to your remarks. Next to Brad is Elaine Manlove, state election Commissioner for state of Delaware. Small wonder. I think you've got a number of -- number of nicknames for the state of Delaware. She's been an election Commissioner for state of Delaware since 2007 and for Newcastle County throughout her vast experience she's seen many changes from both local and state election process. She's overseen Delaware's electronic signature project to allow voters to have registration information transmitted in real-time from the division of motor vehicles to the departments of election in each county. As Commissioner, she's responsible for the Help America Vote Act funds, state suicide voter registration system, 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. She 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, transportation and government administration and election committees. Also a local election administrator for 14 years in the town of Wilton. I'll turn it over to Peggy.

>> Okay. Thank you for inviting us to be part of this conversation on election security. And before I begin my remarks I'm 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're always there for us to attend our local and state conferences, attended and presented at every meeting we've use your quick start guides, checklist, guidelines, 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're also protected with a monitor. Our cybersecurity 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 as well as or agencies to further protect our infrastructure. We're doing real time monitoring of all in bound and out bound 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 the system the local election official must use a workstation 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 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 ransom ware is being put on their local machines? Certainly the state fusion center would be informed of it, but we would not be informed at the state level. Over the next two months we've decided to do enhancements to the voter registration database that will be implemented to enhance user authentication, including a stronger password policy and two factors authentication. Also we will have a new analytics report that will compare voter data over time to look for any anomalies that we're 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 that 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 cybersecurity election system within our office, consisting of an election officer with subject matter experience in technology and cybersecurity and an IT cybersecurity professional who would have subject matter experience in elections. We have also recently created a Connecticut cybersecurity task force composed of representatives from DHS, the Connecticut National Guard, state government legislative and 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're pleased Congress authorized these additional HAVA funds to enhance technology and make election security improvements. We believe that 2018 election will be one of the most challenging elections we've fade but we'll work with our local election officials to make our systems are secure and the public has confidence in the outcome. Thank you.

>> Thank you so much, Peggy.

>> Thank you. Thank you for inviting me to speak today and I want to echo what Peggy said, thank you for 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 as you central place to go to for answers. So the first round of HAVA allowed Delaware to introduce electronic signature, the interface we've faced -- we've made with DMV ream time interface. It also allowed us to do automatic voter registration which was kind of the I guess our e signature was the forerunner to automatic voter registration. Then online voter registration. So we used most of the original HAVA funds to use technology to improve the way we did the way we do our business every day. As we move forward with the new funding, as grateful as we are for this funding, you know, our plates are even fuller now than they were then because of security. So I just want to bring you up to speed 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 the TV seeing everybody with the hanging chad and calling me up saying what a great job Delaware was doing. And now they're saying people are calling saying where is the paper trail? So times change. But as we look at new voting machines, security is of course 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's a process to find new voting machines. I think the general public sees well you don't have a paper trail so let's just go buy new machines as if I can walk into staples and load up a cart. The public we used a lost public input in this, we had a task force 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 DRE with an iPad -- that's the challenge at this moment in time. Thanks to HAVA, I am sure that -- thanks to the HAVA funds I'm sure that will be a part of the funds that buy these new voting machines. We're also look at electronic poll books, something web don't have now. But there's a bill in our legislature now to create early voting and that that will necessitate the poll books. The state, we're on the state's mainframe, and they want us to get off the state's mainframe so we're looking now at election management and voter registration system and we'll look at updating our absent see system although one we have is -- we've bought with HAVA funds and it is fine. So we are different than a lot of other states. Delaware, everybody all the election officials in Delaware are state employees, always have been. We used to have four different agencies, but 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. We work together and meet once a month and review all 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 or department of technology information for providing the security. So we work with them and this new timeframe has allowed me to find out we've always belonged to MS ISAC as far as department of technology, not necessarily elections. We have an Albert monitor I went back from the last meeting and said we need to get this Albert monitor and 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 has gone on that we don't know. As we move forward we're looking at the penetration testing through homeland security and I found out 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're going into. And I think in reality, that works, but in the view of department of technology and information, they want all that addressed in writing so we're back and forth on that right now and I'd like to talk to other states touring the next couple days and see what their experience has been. So again, we're grateful for the additional funding, but again, our plates are even more full than they were because of security. This is a great help to us. Thank you.

>> Thank you, Elaine. Brad? Looking forward to what you have to say

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

>> Thank you.

>> I was also intrigued during the opening remarks made my Commission members that you both mentioned territories in the Pacific Ocean. The smallest U.S. possession is a beautiful tropical island in the South Pacific noted for its scuba diving named king man reef. Unfortunately it has no population so therefore it will not qualify for any grants but I think a voter or even election administrator would have had to 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 focus on one aspect of security that I think is particularly important for county and local election officials. In Indiana we certainly have taken challenges and threats of cybersecurity to state wide voter registration system seriously. Our legislature appropriated funds for modernization of our voting system -- 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 alarm 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 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 that's contained in that inventory is up to date. With that in mind we've

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 for review and approval. We look forward to making certain that the inventory remains constantly current and further, addressed 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 owner counties or jurisdictions throughout the United States. Thank you for the opportunity to speak.

>> Thank you, Brad. I'll start -- I'll start with questions. And you mentioned just now vendors. And mentioned experience you had with a vendor. In general, how have the vendors been? This is an important -- they're 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 -- could they help bridge some of the issues here between states and locals?

>> 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 cybersecurity 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.

>> Do you think they're taking adequate steps to address the cybersecurity and the security, physical security issues?

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

>> Thank you. You have either -- either of the other want to weigh in on that vendor issue?

>> I've been dealing with vendors recently and I've been satisfied with the response. Again, when we talk about adequate as far as security, I never know what adequate is. I think we think we're all at some level, but if the bad guys get to another level, I think that's just an ongoing game that we're going to be playing. And I think -- 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're all in the same game

>> 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's something we all need to talk about. And perhaps have audits of the vendors themselves. You know, where they program the cards, to be sure that that's safe and secure.

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

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

>> So we're mandated to 5% of all of the polling places on a random basis after every election and primary.

>> We have a revision for audits upon request following election.

>> Okay. Peggy, you mentioned Albert sensor. This is one of those questions where we know the answers but not everybody does --

>> I knew you would ask that question. I did write it down a little bit. Because I honestly didn't know before now. So I think it's also called Einstein sometimes, relate? But it's the -- it's a network monitoring system which provides automated alerts of malicious network threats focused on state, local, territorial and tribal and -- so if anything accommodation up et cetera sends to MS ISAC for analysis and then they let us know. I think basically that's what I've been told it is.

>> Thank you.

What would you consider your biggest one or two challenges or risks in this security environment? Each of you. Maybe -- just one or two things that you're most concerned about.

>> Well, again, I think I've 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're such tiny towns in Connecticut they are not staffed every day. The town clerks are there to -- but the town clerks are only involved in issuing absentee ballots so everything else is done by the registrars of voters so my concern is the fact that we have part time people and we have to make sure they are certainly trained on cybersecurity going forward.

>> So maybe some professionalism issues?

>> Yes.

>> Uh-huh.

>> Yes.

>> Elaine?

>> While we're state employees, but I do think making everyone understand from no matter what position you have that cybersecurity affects all of us and making everyone aware of the importance of it and, yes, training and training and training.

>> 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 that we can promptly investigate it and prevent any concern that's unfounded. 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'm seeing something unusual, it may mean nothing, but I'm 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.

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

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

>> 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 marshaled all the forces available to mitigate anything like this. So I think, yes, I have confidence. I have more knowledge than did I before, and, yes more confidence goes with that.

>> Yes, I'll join that statement too 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.

>> Thank you to all of you. That's a question I'm asked often when I'm out. People ask me can we really believe in, you know, 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. Yes. Chairman Hicks?

>> I want to thank you all for being here today. I've known each of you for a number of years and I know that 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've mentioned audit as triggered by request. Who makes that request?

>> The request under Indiana statutes can be made by political party chairs who might anticipate a recount being filed.

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

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

>> You mentioned that the state is asking that you leave their mainframe. What sort of -- do you have an estimate of time frame and cost that's going to be associated with that?

>> Not yet. We're working on that right now and I now have an RFP that we have responses to and part of that is the new election management system. When we get down to the dollars and cents of it we're not there yet. It will happen sooner than later but that's all going to depend on the cost of the voting membrane. Our RFP was four sections, voting machines, election management system absentee and poll books so depending on cost is depending on how fast it all happens.

>> So I guess it's more for all three of you. Are you on the mainframe for your particular state? So, do you have an individual mainframe for your offices?

>> We have a dedicated mainframe.

>> Again, we are on the state's mainframe but working to move off.

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

>> And I only have a couple more questions. Because I believe that there are other events going on today and we have a third panel going on in a bit. But what -- I want to thank you for the praise that you gave to the EAC. As chair it's easy to sit here and try to take credit for that, but it's mostly the staff that we have a very dedicated staff and I'm 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 given the accolades.

But that being said, what more can we do to help you in 2018 and 2020? 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?

>> I would say just keep doing what you're doing. I mean, I took a look at your website, and there's such a wealth of information there. Almost too much. You could spend days looking at everything that 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 just say keep doing what you're doing.

>> And I'll echo that. It is a great place -- we have of a place now to go that we didn't have before 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.

>> In addition to those, I would add continue the efficient manner in which you've begun the process of educate being us about the new funding. Work with us as we

have questions. And I anticipate that we'll be able to use that money in the best interest of the voter. Thank you.

>> Do you have any additional questions? So I want to thank you all the for being a part of this. I've been invited to two of your states and I hope to come and -- I guess every Monday the first Monday of each month and then it's going to be in September, hopefully, that the clerks association is going to have me in Connecticut. So I want to thank you all for being here. And thank you for what you do. And looking forward to seeing you tomorrow with the Standards Board. With that I want to open up for the audience. If you are an election administrator or election person, Natalie from our staff is there and you can line up behind her. We're 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're with, and limit your comments to five minutes. We'll try to get as many -- if you want to use the podium or sit at the seat -- we want to limit it as much as possible. So they want you to use the podium. If you can turn the other two mics off, I think -- if you turn the other two off, that one should come on. There you go. When it turns red. There you go.

>> I can program a voting system, but I cannot operate a microphone. Thank you.

My name is Dwight Shelman [phonetic], 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's 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 this process. Commissioner Hicks asked at the conclusion what more can the EAC do. And I think there's 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, you know, different circumstances in their own individual jurisdictions, but the threats are common. And rather than having 50 states and

territories and, you know, 6,000 local election jurisdictions recreate the wheel on all of these elements, I think there's some commonality that the EAC can provide some resources for. For example, an online cybersecurity training for state and local election officials and poll workers. And I think as Noah pointed out, this is -- we're all as strong as our weakest links, and because of that, you know, 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'm sure there are many other ideas out there. My next plea is to the election integrity advocates. I think it's 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 the 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're all vulnerable. That is absolutely not the case. And then my final plea is a plea to the system 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 center for justice is hosting a panel in the Cadiz room. Room on the mezzanine level, which will be a panel discussion where we can get in the room and maybe talk through some of these issues. The former Secretary of State for Kentucky will be moderating that. Doug Kellner [phonetic] and Liz Howard will be on the panel as I will be as well. And it's 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.

>> That's going to be here in the hotel?

>> Yes. It'll be starting at 4:15 in the Cadiz room. And refreshments will be served. Thank you.

>> Good afternoon, my name is Doug Kellner co-chair of the New York 78 board. I'll join Dwight's invitation for those of you who would like to join us one flight up to continue these discussions. I have submitted a lengthy statement, which I hope will get published eventually, and so I'll just focus on two or three small points that I think have not been discussed so far. The governor 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 and one of the innovative things that was added to New York law was to require disclosure of independent expenditures for internet ads. And 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. And it'll 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. And I think that 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 access 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.

>> Good afternoon. My name is Rob Rock, director of elections for Secretary of State in the state of Rhode Island. I 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 election and is multiply of it we've learned at these type of meetings from other states. When secretary got elected in 2014 and started in 20151 of her top goals was to Maureen elections in Rhode Island. One way is on the cybersecurity front. Just last Wednesday we held a briefing for members of the public and 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 [for] 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 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, governor's office, board of elections, our local election officials which I'd like to take a moment to recognize Louise Fanoff [phonetic] today of the Standards Board. Welcome. Quickly I want to talk about how we're securing our online systems. Secretary of State has taken a variety of measures to greatly reduce mitigate the threat of cyber attacks and one of the ways is partnering with the department of homeland security under the critical infrastructure designation to further protect or central voter registration system by testing for vulnerability, sharing cybersecurity information threat incident reporting and receiving ongoing risk and vulnerability assessments that include penetration testing, web application testing and so social engineering. We're also working with our state's higher education institutions, very fortunate in Rhode Island to have quite a few nationally recognized institutions of higher learning, for example, Brown University, we worked with closely on cybersecurity and computer science matters and they've been great. Having academics at the table has been

helpful for us. We're also working with other state partners such as the National Guard and the state police fusion center who both done assessments on our voting systems and offered recommendations for ways that we can protect ourselves more. It's been great to partner with other state entities because 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, 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 ISO software which meets security requirements for federal government secure network. We also passed in 2017 be an audit law similar to what Dwight and his team successfully launched last year. We have a risk limiting audit law we'll be rolling out over the next few election cycles, which we feel is very important. 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 are a variety of technological expertise and it is imperative local election officials can speak articulately about elections security and helping prevent attacks on our systems. So in 2017 in October we convened the cities and towns for a cybersecurity summit and went over cybersecurity 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 summits. We also within the department of state began a phishing campaign to test 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 our employees are going to be trained on the best practices for cybersecurity. So I'll end with federal state and local government cannot allow cyber threats to election systems will to undermine the role voting plays in our society. Despite the progress made it is important to remember that cybersecurity is not a destination but a continually evolving road that requires constant attention to mitigate risk. Always strive to do better for voters because a single act of casting a ballot is fundamental to making government accountable to the people it serves. It requires a continued commitment and corresponding dedication of

resources to ensure e been integrity of our voting systems. And I apologize for going over my allotted time. Sorry. Thank you.

>> Sure. Thank you so much. While I was sitting here just an observation, you know, 18 years ago this was ground 0. South Florida. In the Bush v. Gore race. How far this election field has come since then. It is remarkable. And I appreciate all the professionalism in this room, the excellent comments and is 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.

>> 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 -- or -- oh, yeah. Or clearinghouse --

>> Clearinghouse@EAC.gov

>> 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)