Meeting Minutes
United States Election Assistance Commission
PUBLIC FORUM ON ELECTION SECURITY IN 2018: Perspectives from State and Local Officials
April 18, 2018

Hyatt Regency Coral Gables
50 Alhambra Plaza
Coral Gables, Florida 33134

The following are the Minutes of the United States Election Assistance Commission ("EAC") Public Forum on April 18, 2018. The forum convened at 2:02 p.m. EDT on Wednesday, April 18, 2018, in Coral Gables, Florida at Hyatt Regency Coral Gables and adjourned on Wednesday, April 18, 2018 at 4:13 p.m. EDT.

Wednesday, April 18

Forum Welcome

Chairman Thomas Hicks welcomed everyone to the United States Election Assistance Commission's (EAC) Public Forum on Election Security in Miami, Florida.

Commissioners' Opening Remarks

Chairman Hicks noted the importance of having discussions on election security and to hear directly from state and local election officials on the topic. He publicly thanked the Congress for the $380 million that was appropriated for the purpose of increasing election security. Chairman Hicks emphasized that today is an opportunity for state and local election officials to offer their concerns and statements on election security.

Vice-Chair Christy McCormick also welcomed the attendees to the forum on election security. She stated that this type of event is very important to the EAC Commissioners and to the staff of the EAC as it helps with the understanding of the issues that face election officials. In addition, these discussions give added perspective regarding how the commissioners and staff can better serve state and local election officials. Vice-Chair McCormick also acknowledged the Trump Administration and the Congress for securing the $380 million in Help America Vote Act (HAVA) funding. Vice-Chair McCormick thanked the EAC staff, including Executive Director Brian Newby and Grants Director Mark Abbott for their efforts in getting the funds out to the various states. She also expressed her appreciation to all of the state and local elections officials and

thanked them for being such serious and dedicated public servants who prioritize the conduct of well run, secure and fair elections.

Vice-Chair McCormick also emphasized that the administration of elections has changed dramatically over the past eighteen years, especially during the last two years. She stated that election security is now in the forefront of the minds of all election officials, and she looks forward to hearing from a few of them during today's forum. She then invited Executive Director Brian Newby to make some opening remarks.

Executive Director Brian Newby provided some background related to the idea of sponsoring the forum. He stated that the desire was to provide an opportunity for election officials to speak about their thoughts concerning election security. The discussion would be for elections officials and by election officials. Mr. Newby reminded everyone that the EAC provides several resources on best practices on its website, EAC.gov. He also stated that the EAC has created a video that officials can show to civic groups, rotary clubs and other interested parties to explain how election security works.

New Help America Vote Act (HAVA) Election Security Funds

Mark Abbott, Grants Director for the EAC, provided an overview of the process required for jurisdictions to apply for and receive HAVA funds which were recently provided by Congress. From a historical perspective, the most recent HAVA funds were appropriated by Congress eight years ago. Prior to this, in 2003, HAVA funding was made available for jurisdictions to improve the administration of elections. There was considerable flexibility regarding how jurisdictions could spend these funds.

Approval of the current appropriation occurred when it was signed by the President on March 22, 2018. Mr. Abbott explained that the funds need to be drawn down and expended by the jurisdictions by 2023.

Award packets were issued to the jurisdictions on April 17, 2018. These award packets have three parts. The first is a Notice of Grant Award which allows jurisdictions to access the fund and gives them the requirements that must be followed to draw down and spend the funds. It also provides instructions regarding obtaining the funds from the United States Treasury. Jurisdictions have 90 days to draft a plan explaining how it intends to spend the funds. These plans will be posted on the EAC website for reference purposes. The EAC will provide some technical assistance to the jurisdictions in the preparation of these plans. Mr. Abbott reminded everyone that the funds can be accessed prior to the preparation of the plan. The funds are available immediately and must be

used to improve the administration of federal elections, including enhancing technology and making security improvements.

Regarding the improvement of the administration of federal elections, Mr. Abbott stated that the funds can be used for education and training, equipment, voting systems and technology, as well as methods for casting and counting ballots. The funds can also be used to improve accessibility and the quality and quantity of polling places.

Mr. Abbott stated that the EAC has received many good ideas from various jurisdictions related to how the funds will be spent. He committed to posting those ideas on the EAC website and encouraged people to share those types of ideas with the EAC.

Mr. Abbott will be available throughout the conference to answer questions.

The floor was then opened for questions.

Chairman Hicks noted that the President signed the funding bill on March 22, and asked when the money is available to jurisdictions. Mr. Abbott noted that the funds were available on April 17, 2018. He also noted that the jurisdictions must follow a five-step process to access the funds. The timing of the draw down of the funds from the United States Treasury is up to the various jurisdictions, so long as this is done within five years.

Chairman Hicks then asked when the 90-day period for issuing their narrative plan began? Mr. Abbott stated that the 90-day period began on April 17, 2018. He believes that would make the deadline July 15 or 16, 2018.

Chairman Hicks mentioned that Congress has stated that the funds should be used to purchase new voting equipment, and that the equipment must adhere to the law regarding providing those with disabilities the ability to vote independently and privately. He then asked about what restrictions have been placed for the use of the money? Mr. Abbott stated that Chairman Hicks was correct. The funds are to be used on security. Congress left the decision regarding what type of equipment to by to the various jurisdictions.

Mr. Newby mentioned that the WAC will attempt to move the funds out to the jurisdictions in as timely a manner as possible, and that the important thing to remember is that there are very few restrictions on the use of the funds.

Vice-Chair McCormick asked for clarification on the amount of disbursement of funds to all of the states and territories. Mr. Abbott stated that the states will receive a minimum of $3 million each, and that the territories, other than Puerto Rico will receive $600,000 each. The states do have a matching requirement, but the territories do not.

Vice-Chair McCormick mentioned that there was a 5 percent matching requirement, and asked Mr. Abbott to provide an outline of that match. Mr. Abbott stated that adjustments to the appropriation were made in two ways. The first was that there was what was considered one-year money. This money must be spent within five years, and the jurisdiction must provide a 5 percent match. The matching funds can be provided over a two-year period. The matching funds can be in the form of cash or an in-kind contribution.

Mr. Abbott then discussed the audit obligations that exist regarding the spending of the funds. He stated that his office will be available to aid jurisdictions with support and technical assistance both before and after the completion of the audit. Mr. Abbott also mentioned that the audit standard is found in the OMB Circulars which informs the jurisdictions what types of expenditures are allowable and not allowable when spending federal money. He further explained that expenditures which are not provided for in the three-page narrative plan will be questioned by the audit.

Vice-Chair McCormick asked if the narrative statements can be updated. Mr. Abbott said they can be updated as needed.

Vice-Chair McCormick then asked what happens to any funds that have been drawn down but not spent within the five-year time limit? Mr. Abbott stated that there is an expectation that the funds will be expended within the five-year time limit. The possibility of an extension can be explored if the money is needed beyond the five years. Mr. Abbott further explained that the requirements for spending these funds are not as flexible as was the case in the past.

Vice Chairperson McCormick thanked Mr. Abbott and encouraged people to contact him to ensure that the funds are spent appropriately.

Chairman Hicks thanked Mr. Abbott and Mr. Newby. Chairman Hicks asked for confirmation that the EAC will be holding several conference calls and webinars over the next few months to assist officials going forward. Mr. Abbott stated that all that information will be on the website.

Election Cybersecurity Update from the Perspective of Local Election Officials

Chairman Hicks introduced the panel discussing election cybersecurity from the perspective of local election officials.

Chairman Hicks introduced Lance Gough, the Executive Director of the Board of Elections for Chicago, Illinois. As Executive Director, Mr. Gough has for the last three decades been responsible for managing voter registration and election administration for 1.5 million voters. Mr. Gough oversaw the recruitment and training of 2,000 high school poll workers and the implementation of the first utilization of electronic poll books in every precinct. He lobbied successfully for on line voter registration, election day registration and on-line ballot access for use by military personnel and overseas voters.

Chairman Hicks then introduced Ricky Hatch, the Clerk Auditor for Weaver County, Utah. Ricky was honored by his fellow county auditors as Utah's Auditor of the Year in 2015. Previously Mr. Hatch worked as an Information Systems Auditor and a consultant for Price Waterhouse. He also was employed as a business analyst and project manager for Parametric Technology Corporation.

Chairman Hicks introduced Noah Praetz, Director of Elections for the Cook County Clerk's Office in Chicago, Illinois, one of the largest jurisdictions in the country. Each year his team services 1.5 million voters and facilitates democracy for thousands of candidates. Mr. Praetz began his career as a temporary worker in 2000, becoming Deputy Director of Elections in 2007 and Director in 2013. He is a board member of the International Association of Government Officials. He has previously made presentations on election day management, on-line registration, voter registration modernization and other election related issues.

Lastly, Chairman Hicks introduced David Stafford, the Supervisor of Elections for Gambia County, Florida. He was elected to that position in 2004 and is the co-chair for the CSG Overseas Voter Initiative Policy working group. He is a board member of the National Advisory Board Elections Systems and Software and a member of the Technology and Elections Working Group for the United States Elections Assistance Commission. He previously served as the northwest Florida Director for United States Senator Connie Mack and as chief of staff to United States Congressman Joe Scarborough.

Mr. Gough began his presentation by describing the many changes that have occurred over the past years in the administration of elections. Clearly, the newest challenges relate to the need to maintain the public's

faith in the security of our elections. This is illustrated by the 2016 incident where Russians hacked into the Illinois State Board of Elections voter registration database. Mr. Gough emphasized that this incident had no effect on individual's voting records. Though this incident had no effect on balloting systems, it did undermine the faith in the voting franchise. Additionally, in 2017 a vendor who was working on electronic poll books exposed voter data to the public. Though none of the data got out this incident made it clear that more is needed to be done to control voter data to ensure that if someone were to attempt to hack into the system nothing could be done with it. Mr. Gough's office is currently going over security procedures with vendors. All data made available to outside vendors and others is going to be significantly reduced. He wants to make sure that his office is prepared and that nothing will get out should future incidents occur.

Mr. Hatch remarked that the biggest cyber security hurdle facing election officials is not technology, but it is building and maintaining public trust. Recent opinion polls show that 71 percent of Americans trust their local government to handle problems, while only 62 percent trust their state government. The number drops to a dismal 31 percent who trust the federal government. Trust starts locally. It is the same with elections. The closer the election is to home the more likely it is to be trusted. A voter's trust in the nation's election process is driven by the voter's experience with their local election office. The challenge is the fact that the level of government that the voters trust the most is also the level that has the fewest resources. It needs to be recognized that the local election officials need to be the face of elections to people, but those local officials need the funding to do the job right. The challenge is to figure out how to support the local officials with the training, technology and funding they need to ensure that their house is in order. One way to do this is to ensure that the federal HAVA funds don't all stop at the state level, but that they also flow to the local election officials. These funds will help local election officials properly implement cybersecurity tools and help to strengthen the public's trust in our nation's election infrastructure.

Mr. Praetz stated that the national security community warns us to expect more sophisticated and evolving attacks. He stated that local officials are on the front lines, facing down powerful and shady adversaries. These same local officials are pressing for resources however. There is a need for better technology, and top-notch personnel with skills to navigate the cyber mine field. His office has tried to take the lead on technology and security by using applied forensics in elections. They published the first white paper written by election officials in the wake of the 2016 attacks. His office worked with the Center for Internet Security and the Defending Digital Democracy Program at Harvard University's Belfer Center to help adapt their digital expertise to the unique context of elections. It has

become crystal clear that local election officials need one person to take ownership of security in each election office. The recently released $380 million in HAVA funds is a very important start, but it may be necessary to invest that much annually. The top priorities for funding include the handful of states and counties that still have paperless voting systems. There needs to be an army of digital defenders who will serve election officials. These digital defenders would improve defenses within election offices, work with outside vendors to eliminate or defend specific vulnerabilities and build a culture of security that adapts to the evolving threats we face. These dangers are not hypothetical and successful attacks may not change a single vote, but it could still damage public confidence. A new digital breach could turn sore losers to cynicism, disbelief, and even revolt. We can't eliminate every chance of breach, but we can make successful attacks rare.

Mr. Stafford spoke about the activities of the Government Coordinating Council (GCC) and their work with the Department of Homeland Security (DHS). The GCC was formed only nine months after Secretary Johnson declared elections as critical infrastructure. A working group was established to develop a communications protocol allowing the work between the federal, state and local partners to be shared. In addition, there was a pilot that was established in testing the multi-state ISAC for elections infrastructure. The pilot was deemed to be successful. As a result, 47 states, 376 local election officials and three associations are now members of the EI-ISAC. Mr. Stafford stated that he believes the relationship between the Department of Homeland Security and state and local election officials has improved. The various officials have begun to work together and there is a level of trust that continues to build. There are a significant number of local election officials that are on the front lines and the communications process is very important. Great progress is being made in communicating and determining what type of information needs to be shared. Mr. Stafford offered a word of caution regarding statutory language. As an example, the audit provision would require 22 percent of the ballots in his jurisdiction during the 2016 election to be subject to audit. That is a high standard. It is questionable whether that level of specificity should be enshrined in statutory language. In Florida, the legislature approved funding to allow counties to acquire network monitoring devices. Election supervisors have attended recent EAC provided training. A recent conference devoted an entire day to cybersecurity with officials from DHS, the FBI and the National Guard among others. We are working hard to ensure we are in the best possible position for the 2018 elections and beyond.

Chairman Hicks thanked the panelists for serving as local election officials and reiterated their importance by remembering Wendy Noren, an election official who recently passed away. The Chairman remembered Ms. Noren

as 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.

Chairman Hicks addressed a question to Mr. Hatch by acknowledging that Mr. Stafford mentioned a 22 percent audit requirement. What is a typical number for audits overall? Mr. Hatch replied that typically in financial audits a sample size of 60 provides sufficient coverage, but elections officials need to be held to a higher standard.

Chairman Hicks mentioned that the EAC has put together a program that discusses basic IT management with local elections officials. He asked the panelists to discuss the role that poll workers can play in terms of election security.

Mr. Stafford responded by stating that the University of West Florida has a Center for Cybersecurity and provided his staff with in depth training on cybersecurity. There have been efforts to determine if such training can be provided to state and local officials.

Mr. Hatch stated that the Department of Homeland Security has many resources and have pledged to offer help to officials from both large and small jurisdictions.

Mr. Gough mentioned that there is a wide diversity in terms of the size of election jurisdictions and help needs to be provided, especially to the smaller jurisdictions, as those are the jurisdictions that are going to be attacked.

Mr. Praetz also mentioned the varying sizes of jurisdictions and that all are subject to attack. None of the organizations have full blanket coverage against attack. Mr. Praetz stated his firm belief that this challenge can only be answered with the addition of people that have the capacity to accept a threat and then to work through all the free resources that are available.

Vice-Chair McCormick also thanked the panelists for their service and mentioned that the one silver lining to what happened in 2016 is the focus that is now being placed on these problems. Ms. McCormick asked what could happen if someone were to get into the system?

Mr. Gough stated that it depends on what type of system is broken into. There is a back-up signature book, paper, should electronic poll books be shut down. Paper based systems can back up electronic systems. It would be very hard to get in and hack the actual vote counting because

there are so many different pieces of equipment in use. It is the election database that is vulnerable.

Vice-Chair McCormick mentioned that there are voter registration systems, voting systems, tabulation systems and election night reporting systems. Do we look at those systems separately or do we look at them as a whole?

Mr. Stafford stated that it is important to understand that voting systems and election systems are not the same thing. Previously the focus has been on traditional election security, including polling place security, ballot security and the security of voting equipment. There will always be issues with this type of physical security. We must be careful in the words used to describe a hacked election versus what are the normal ebbs and flows of an election cycle.

Vice-Chair McCormick asked panelists to expand on some of the challenges in communicating risks and threats, and what local officials can do without adequate funding in regards to security?

Mr. Hatch responded by saying that you want to foster as much communication as possible while respecting the different positions and levels involved in the communication. Sometimes the various entities that must communicate with each other lack trust regarding each other's motives. It is important to understand what types of information need to be communicated and who to communication that information with. Mr. Hatch stated that the draft communication document he is working on should be out soon. The GCC has looked at it, as has the DHS. The document is relatively general, but Mr. Hatch hopes it will be helpful.

Mr. Praetz stated that his suggestion is that local election officials should work with a digital defender and take the CIP or Belfer documents and bring their elections security systems, primarily their digital tools and internet tools, up to date as quickly as possible.

Vice-Chair McCormick noted that many local election offices operate with only one person. What one or two pieces of advice would you give them on how to secure their offices?

Mr. Hatch stated that we must have a secure mindset. Security doesn't just relate to voter machines and voter systems, but also to personal Facebook accounts, email, because that tends to be overlooked.

Mr. Stafford mentioned that the human firewall is very important. Statistics show that between 80 and 90 percent of all attacks are initiated through email. Try to address that concern.

Mr. Gough stated that there are many state organization that are reaching out to the local, small jurisdictions with help.

Election Cybersecurity Update from the Perspective of State Election Officials

Vice-Chair McCormick thanked the panel members for participating. She also invited anyone who wished to provide a written statement to do so. The statement can be submitted electronically at clearinghouse@eac.gov. The statements will all be read and possibly posted on the EAC website. Ms. McCormick then introduced the panel of state election officials.

The first panelist is Brad King, who is the co-Director of the bipartisan Indiana Election Division, which provides information regarding the election process, campaign finance, voter registration, absentee voting and other duties in state election administration. Brad has served as a senior staff attorney for the Legislative Services Agency and counsel to the Indiana House and Senate Elections Committees. He has also served as Assistant Cooperative Counsel for the city of Indianapolis, counsel to the Marion County Board of Voter Registration and State Elections Director for the Secretary of State of Minnesota.

The second panelist is Elaine Manlove, who is the State Election Commissioner for the state of Delaware. Elaine has been an Election Commissioner for the state of Delaware since 2007. Previously, she spent eight years as the Director of the Department of Elections for New Castle County. She has seen many changes from both the local and state process. Elaine has overseen Delaware's electronic signature project and is responsible for the Help America Vote Act funds, the statewide voter registration system, campaign finance and the parent-student mock election.

The final panelist is Peggy Reeves, who is Assistant to the Secretary of State for Elections in Connecticut. She was appointed Director of Elections for the Connecticut Secretary of State's Office in 2011. Previously she served in Connecticut's General Assembly as a state representative, representing the towns of Wilton and Norwalk, where she was a member of the judiciary, transportation and government administration and election committees. Peggy was a local election administrator for 14 years in the town of Wilton.

Ms. Reeves opened the discussion by thanking the commissioners and staff of the EAC for all the resources and help that EAC has provided, and she expressed her hope that one or two additional EAC commissioners will be appointed soon. Ms. Reeves stated that she was surprised to

learn last fall that Connecticut was one of 21 states that was targeted by the Russian government. The security defenses held, and the Russians were turned away. Connecticut officials are now leveraging the services of DHS and other agencies to further protect their infrastructure. She stated that they are doing real time monitoring of all inbound and outbound traffic to the state network, conducting hygiene scans of internet facing applications and will be having a risk and vulnerability assessment conducted by DHS next week. As an additional level of security, Connecticut's centralized voter registration system is not directly connected to the internet. The state of Connecticut is highly decentralized as it does not have county governments. Accordingly, elections are run by 338 registrars of voters and 169 town clerks. If you add the deputies and assistants, there are several thousand local election officials in Connecticut. While this decentralized system makes it difficult for systems to be hacked, it is also a weakness because of the diverse systems which exist and access to the centralized voter registration system. Over the next two months enhancements are to be implemented to enhance user authentication. In addition, there has been an increasing need for a marriage between IT staff and election staff, so the decision has been made to create a cybersecurity election system within the office. Ms. Reeves states that they are pleased that funds are being provided to enhance technology and to make election security improvements.

Ms. Manlove also expressed her appreciation for the work performed by the EAC. She stated that previous HAVA money has been used in Delaware to introduce electronic signatures and on-line voter registration systems. Though grateful for the new HAVA funds, Ms. Manlove stated that the needs in Delaware are great. New voting machines are needed. Previous HAVA funds were used to purchase paperless voting machines, which at the time were the latest in technology. Currently, machines with paper trails are expected, so times do change. In addition to voting machines, it is expected that the new HAVA funds will be used to purchase electronic poll books and election management and voter registration systems. Delaware is also looking to update its absentee system. Delaware was one of the 21 states where there was an attempted intrusion, and Ms. Manlove is grateful to the Delaware Department of Technology for providing the necessary security. She is confident in the security of Delaware's election system, but each day presents different challenges.

Mr. King also expressed his appreciation for the work conducted by the EAC, particularly regarding voting systems. Mr. King stated that Indiana has taken the challenges and threats to the statewide voter registration system very seriously. There are also physical security protocols that need to be undertaken in counties who maintain voting systems. Indiana passed Public Law 100 which 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 alarm systems and video cameras. The legislation also sets forth very detailed protocols regarding chain of custody, ceiling and other items regarding the physical management of voting systems, but recognizes that not all counties are the same. Mr. King also stated that counties are not required to submit a voting system or electronic poll book disposal plan to the state for review and approval.

Vice-Chair McCormick began the question and answer period by stating the vendors are an important partner in the election community. We usually don't hear from vendors in this type of a setting. What have your experiences been recently with vendors?

Mr. King stated that vendors do play a key, pivotal role in the security process for the voting systems. He said that his experience is mixed, particularly regarding poll book vendors, which is a growing industry. The education process regarding cybersecurity threats and physical threats is important, not just for elections officials but for vendors as well. Vendors seem to overall have a desire to cooperate and help improve the system.

Vice-Chair McCormick asked if vendors are taking adequate steps to address cybersecurity and the physical security issues?

Mr. King responded by saying that he is not confident that all vendors are fully addressing all cybersecurity concerns.

Ms. Manlove stated that she has been satisfied with their response. She mentioned that cybersecurity is always changing and is attempting to keep up with the bad guys. She believes that the vendors are working with state officials.

Ms. Reeves responded by stating that vendors in the past have been focused on physical security, such as strict chain of custody and programming, but not as much on cybersecurity. Ms. Reeves thinks that perhaps there is a need to have audits conducted of the vendors.

Vice-Chair McCormick asked if any of the represented states conduct audits and if so, what do those audits look like?

Ms. Manlove stated that Delaware has random audits conducted but nothing is mandated, but she expects that may be the case moving forward.

Ms. Reeves noted that Connecticut requires an audit of five percent of all polling places on a random basis after every election and primary.

Mr. King stated that Indiana has a provision for audits upon request following an election.

Vice-Chair McCormick asked what an Albert Sensor is?

Ms. Reeves responded that it is a network monitoring system which provides automated alerts of malicious network threats focused on state, local, territorial and tribal jurisdictions. If anything comes up, it is sent to MS-ISEC for analysis and they make us aware of the issue.

Vice-Chair McCormick asked each of the panelists to provide one or two challenges or risks in this security environment that we should be concerned about?

Ms. Reeves stated her concern that many of the local election officials in Connecticut work on a part time basis. The sizes of the jurisdictions are so small that the officials may not work every day. There is a concern that part time staff are not adequately trained on cybersecurity.

Ms. Manlove stated that her concern is making everyone understand that cybersecurity affects us all. Everyone must be aware of the importance of it.

Mr. King mentioned that his concern is with the chain of communication. So often we discover an issue only after it has become a public issue or public question. We encourage the vendors and county election officials to inform us immediately of any anomaly, so we can promptly investigate it and address any concern. We need to empower the poll worker to ask questions.

Vice-Chair McCormick asked, recognizing that incidents have and will occur, can our voters have confidence in the security of our elections?

Ms. Reeves stated that yes, they should. No votes changed in 2016. They should have faith in the fact that we are moving forward to make sure that we do the best we can to make sure nothing happens to jeopardize 2018 and 2020.

Ms. Manlove commented that she agrees. 2016 was a wake-up call for all of us. We have more knowledge than we did before and more confidence.

Mr. King also agreed the he has full confidence that the elections we conduct are as secure as we can make them. 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.

Chairman Hicks thanked the panelists for participating today. He then asked Mr. King, based on his mentioning audits can be triggered by request, who can make such a request?

Mr. King answered that the Indiana statutes state that the request can be made by political party chairs who might anticipate a recount being filed.

Chairman Hicks asked Ms. Manlove if she had an estimate of the cost and timeframe surrounding Delaware's request that her office not be connected to the Delaware mainframe.

Ms. Manlove stated that this is being worked on. There is an RFP and there have been responses to the RFP. The main concern is the cost of the voting machines. The cost may drive the timeframe.

Chairman Hicks then asked all the panelists if they were on the mainframe of their particular state, or if each have an individual mainframe for their sites?

Mr. King state that Indiana has a dedicated mainframe.
Ms. Reeves stated that they have a server all within the state's service. It is in the same area as the state police, so she believes they are well protected.

Chairman Hicks thanked each of the panelists for the kind words they expressed towards the EAC during their opening remarks and stated that it is a credit to the staff of the EAC. He then asked each panelist what more the EAC can do for them?

Ms. Reeves asked the EAC to keep doing what it is currently doing. She referred to the wealth of information that is available on the EACs website. She hopes that the word can get out to local election offices just how valuable EAC is to the election process.

Ms. Manlove agreed with Ms. Reeves and stated that the EAC is a great asset for all of us.

Mr. King also agreed and asked the EAC to continue the efficient way you have begun the process of educating everyone about the new HAVA funding.

Chairman Hicks thanked the panelists for their participation.

Open Comments Related to Cybersecurity

Chairman Hicks then opened the floor to any election administration or election official for comment.

Mr. Dwight Shellman thanked the commissioners for hosting the forum. In response to the question of what more can the EAC do, Mr. Shellman suggested on-line cybersecurity training for state and local election officials as well as for poll workers. Mr. Shellman then asked election integrity advocates to understand that technology is very important and valuable to voters, but it also introduces certain vulnerabilities and officials must make sure these vulnerabilities are mitigated. Mr. Shellman's final plea was to system providers. He hopes they understand that they are providers of critical infrastructure and trust applies to them as well. He also stated that there will be a forum immediately after this forum by the Brennan Center for Justice on the mezzanine of this hotel. Trey Grayson, the former Secretary of State for Kentucky will be monitoring. Doug Kellner of New York and Liz Howard, formerly of Virginia, will join Mr. Shellman on the panel.

Doug Kellner, co-chair of the New York State Board of Elections repeated the invitation made by Mr. Shellman to participate in the panel later this afternoon. He also mentioned that he has submitted a written statement to the commissioners, and that Governor Cuomo of New York has been very proactive in recognizing security threats which have been a priority in the state budget. New York has added a law that requires disclosure of independent expenditures for internet ads. In addition, there is a need for voter verifiable paper audit trails. There was a recent court decision in New York which allows people to obtain copies of ballot images which will allow voters to do their own audits, which should improve transparency and verifiability.

Rob Rock, the Director of Elections for Secretary of State Nellie Gorbea of Rhode Island, addressed the commissioners and thanked them for hosting this forum. His comments related to what Rhode Island is doing to secure elections. They are working collaboratively with the general assembly, the governor's office, the board of elections, and local election officials to reduce and mitigate the threat of cyber-attacks. Rhode Island is working with the Department of Homeland Security to further protect our central voter registration system by testing for vulnerability, sharing cybersecurity information threat incident reporting, and receiving ongoing risk and vulnerability assessments. Mr. Rock also stated that Rhode Island works with local institutions of higher education, the National Guard and the State Police Fusion Center to determine ways that will further promote cybersecurity. Rhode Island has recently purchased new voting equipment with paper ballots. Rhode Island also works to make sure all local election officials have the knowledge to help prevent threats and assess problems.

Commissioners' Closing Remarks

In her closing remarks Vice-Chair McCormick reminded everyone how far the elections community has come in the past 18 years since Bush v Gore. She stated that she appreciates all the professionalism that is in the room. She also thanked everyone for the excellent comments and questions that were received during the day, and again thanked everyone for their hard work and continued dedication as public servants to our representative democracy.

Chairman Hicks closed the forum by thanking everyone for attending and that any written statements can be submitted and will become a part of the official record. Those statements can be sent to clearinghouse@EAC.gov.

Conclusion

[The April 18, 2018 EAC Public Forum on Election Security adjourned at 4:13 p.m. EDT]